ACTA ARITHMETICA
181.3 (2017)

The main conjecture of Iwasawa theory for elliptic curves with complex multiplication over abelian extensions at supersingular primes

by

Byoung Du Kim (Wellington) and Jeehoon Park (Pohang)

Contents

1. Introduction. Let F be a number field, E an elliptic curve over F, p a prime number, and F_∞ a $\mathbb{Z}_p$-extension. Let Λ be the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$ which we identify with the power series ring $\mathbb{Z}_p[[T]]$. One of the main goals of Iwasawa theory is understanding the close relationship between the Selmer groups of E over F_∞ and the p-adic L-functions of E. As we will see soon, this depends on the reduction type of the primes above p.

When E/F has good ordinary reduction at every prime above p, we have a well-established theory of the conventional Selmer group $\mathrm{Sel}_p(E/F_\infty)$

2010 *Mathematics Subject Classification*: Primary 11G05, 11R23; Secondary 11G40.
Key words and phrases: Iwasawa theory, elliptic curves, complex multiplication, main conjecture.
Received 12 September 2016; revised 3 July 2017.
Published online 1 December 2017.

DOI: 10.4064/aa8606-8-2017

(see [8]). Furthermore, when $F = \mathbb{Q}$, Mazur and Swinnerton-Dyer [17] constructed a p-adic L-function $L_p(E/\mathbb{Q}, T) \in \Lambda \otimes \mathbb{Q}_p$ interpolating the special values of L-functions of E twisted by the Dirichlet characters of p-power conductor. They conjectured that for the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$, the characteristic ideal of $\mathrm{Hom}(\mathrm{Sel}_p(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by $L_p(E/\mathbb{Q}, T)$. This conjecture is commonly called the *main conjecture of Iwasawa theory*. When E has complex multiplication, the conjecture was proved by Rubin [21], and when E does not have complex multiplication, one divisibility was proved by Kato [13]. Both proofs use the Euler system technique. More recently, Skinner and Urban [28] proved the other divisibility, and thus completed the proof of the main conjecture of Iwasawa theory for elliptic curves defined over $\mathbb{Q}$ (assuming they have good ordinary reduction at p).

When E has good supersingular reduction at any prime above p, the picture is much more complicated. It has been noted that $\mathrm{Sel}_p(E/F_\infty)$ and $L_p(E/F, T)$ for a supersingular prime p do not have nice properties of the good ordinary reduction case even when they can be constructed at all in a meaningful way. For example, (for a supersingular p) $L_p(E/\mathbb{Q}, T)$ constructed by the method of [17] is not an integral power series in Λ, but rather a power series with an *admissible* growth rate, and $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)$, whose definition is not contingent on the reduction type of p, is not a cotorsion Iwasawa module. And this is by no means an exhaustive list of problems.

Among alternatives, the plus/minus Iwasawa theory (and its more recent generalization, Sprung's $\sharp/\flat$ Iwasawa theory) seems particularly promising. This theory has been studied extensively for an elliptic curve E defined over $F = \mathbb{Q}$. Pollack [18] constructed plus/minus p-adic L-functions $L^\pm(E/\mathbb{Q}, T) \in \Lambda \otimes \mathbb{Q}_p$ satisfying certain interpolation propeties, and Kobayashi [16] the theory of the plus/minus Selmer groups $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty)$. Similar to the main conjecture of Iwasawa theory, Kobayashi conjectured that the characteristic ideal of $\mathrm{Hom}(\mathrm{Sel}_p^\pm(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by $L^\pm(E/\mathbb{Q}, T)$, which we will refer to as the main conjecture of Iwasawa theory for supersingular primes or *Kobayashi's conjecture*. Pollack and Rubin [19] proved Kobayashi's conjecture when $E/\mathbb{Q}$ has complex multiplication, and Kobayashi [16] proved one divisibility when $E/\mathbb{Q}$ does not have complex multiplication.

Since this paper was written some time ago, much progress has been made in the direction of formulating and proving main conjectures of Iwasawa theory for supersingular/non-ordinary reduction under various assumptions. Iovita and Pollack's [12] generalization of Kobayashi's $\pm$-Iwasawa theory to any ramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ predates our work. Sprung's $\sharp/\flat$-Iwasawa theory ([29], [30]) expands the scope of the theory to the case where $a_p \neq 0$, and he formulates a more general conjecture. Recently, Xin Wan [33] claimed

a proof of the main conjecture of $\pm$-Iwasawa theory (see also Sprung's [31] claimed proof for $a_p \neq 0$).

Also, Büyükboduk and Lei ([2], [3]; see also [1]) have formulated main conjectures of Iwasawa theory for abelian varieties with non-ordinary reduction under some conditions, and for abelian varieties with complex multiplication, they have proved the conjectures. It should be noted that their method is different from ours.

The goal of the present paper is to prove an analogous result when E is defined over an abelian extension F of an imaginary quadratic field K, and has complex multiplication by K, for which a precise formulation of the main conjecture of Iwasawa theory has not been known previously. By Shimura's well-known theory of complex multiplication [26], there is a Hecke character ψ of F associated to E.

In addition, assume $F(E_{\mathrm{tor}})$ is an abelian extension of K. This last condition is fairly common in this area (see for example [6, Section 4.2]), and is equivalent to the existence of a Hecke character φ of K of type $(1,0)$ such that

$$\psi = \varphi \circ N_{F/K}$$

(see [26, Theorem 7.44]). Let $\mathfrak{f}$ be an integral ideal of K divisible by both $\mathrm{cond}(F/K)$ and $\mathfrak{f}_\varphi := \mathrm{cond}(\varphi)$. Let $K(\mathfrak{f})$ denote the ray class field of K of conductor $\mathfrak{f}$. Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F.

Suppose p is an inert prime in $K/\mathbb{Q}$ which splits completely in F/K. Additionally assume that every prime of F above p is inert over $K(\mathfrak{f})/F$. Let R_p be the ring of integers of the p-adic completion of $K(\varphi, \bar{\varphi}, \mu_d)$ where $d := [F : K]$. Let $\Lambda_{R_p} := R_p[[\mathrm{Gal}(F_{\mathrm{cyc}}/F)]]$, which we identify with $R_p[[T]]$. For an R_p-module M, let $M^\vee$ denote the Pontryagin dual $\mathrm{Hom}_{R_p}(M, R_p \otimes \mathbb{Q}_p/\mathbb{Z}_p)$.

In Section 4 we will construct plus/minus p-adic L-functions $L_p^\pm(E/F, T) \in \Lambda_{R_p}$ which have properties similar to the plus/minus p-adic L-function of [18]. We have the following:

THEOREM 1.1.

(1) $\mathrm{char}_{\Lambda_{R_p}}((\mathrm{Sel}_p^-(E/F_{\mathrm{cyc}}) \otimes R_p)^\vee) = (L_p^+(E/F, T))$.

(2) $\mathrm{char}_{\Lambda_{R_p}}((\mathrm{Sel}_p^+(E/F_{\mathrm{cyc}}) \otimes R_p)^\vee) = (L_p^-(E/F, T))$ *if* $\varphi(p) \not\equiv p \pmod{p^2}$.

(Our $L_p^\mp$ corresponds to $L_p^\pm$ of [19].)

To obtain this, we should do more than simply adapt Pollack and Rubin's techniques. At the theoretical level we have two tasks:

- We need to find the plus/minus universal norms which are essential for the theory of the plus/minus Selmer groups (Section 2).
- We need to construct the plus/minus p-adic L-functions of E/F (Section 4).

It is not known, in general, how to generalize the plus/minus Iwasawa theory when F is not $\mathbb{Q}$, although there are some noteworthy cases in which this is known (notably, Iovita and Pollack's work [12] and Büyükboduk and Lei's work [2], [3]). Büyükboduk and Lei had a broader aim of working with abelian varieties in general. Their use of Wach modules enabled them to avoid using formal groups.

Whether $F = \mathbb{Q}$ or not, at some crucial point, we should evaluate the Coates–Wiles derivatives of the elliptic units. However, when $F \neq \mathbb{Q}$, this evaluation is harder because the elliptic units and the elliptic curve E are not invariant under the action of $\mathrm{Gal}(F/K)$. The readers can see in Section 3 how we solve this problem.

The readers who are not familiar with the plus/minus Iwasawa theory might find the following corollary of Theorem 1.1 helpful. By the control theorem for the plus/minus Selmer groups [14, Lemma 4.21], Theorem 1.1 implies the following: Let F_n be the subfield of F_{cyc} with $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$, and let χ be a primitive character of $\mathrm{Gal}(F_n/F)$. Let $\mathrm{ST}(E/F_n)_p$ denote the p-primary part of the Shafarevich–Tate group of E over F_n.

Corollary 1.2. *If n is 0 or odd, then $E(F_n)^\chi$ and $\mathrm{ST}(E/F_n)_p^\chi$ are finite if and only if $L(E/F, \chi, 1)$ is non-vanishing. The same result holds for n even if $\varphi(p) \not\equiv p \pmod{p^2}$.*

Kitajima and Otsuki [15, Proposition 3.4, Remark 3.5, and Lemma 3.6] have made great efforts to remove conditions such as $\varphi(p) \not\equiv p \pmod{p^2}$ above. Their work may not be immediately applicable to our situation because our formal group has a different Honda type $t^2 - \varphi(p)$. However, we hope that with more work we will be able to obtain a result similar to theirs.

2. Formal groups and plus/minus universal norms. Although Fontaine's theory of smooth formal group schemes might be better suited for our purposes, we follow the strategies and notation of the first author's [14], which means we will use Honda's theory of formal groups. (We will not discuss Honda's theory here. Refer to [10] or [16, Section 8].)

Throughout this section we fix a prime p. In this paper, a *formal group* is always a one-dimensional commutative formal group defined over a local field of residue characteristic p. For simplicity, for a formal group F and a local field L, we let $F(L)$ denote $F(m_L)$ for the maximal ideal m_L of the ring of integers of L.

2.1. Lubin–Tate group and explicit reciprocity. We briefly review the (relative) Lubin–Tate group, Coates–Wiles derivative, and explicit reciprocity of Lubin–Tate groups of Wiles.

Let k be a finite extension of $\mathbb{Q}_p$ and let q be the order of the residue field O_k/p_k. (In this section, p_k will denote the prime ideal of k.) We let k^{un} be

the maximal unramified extension of k, and let Fr denote the qth Frobenius on k^{un} characterized by $\mathrm{Fr}(x) \equiv x^q \pmod{pO_{k^{\mathrm{un}}}}$ for every $x \in O_{k^{\mathrm{un}}}$.

Let k' be the unique unramified extension of k of degree d.

We let O' and p' denote $O_{k'}$ and $p_{k'}$. Let π be a uniformizer of k' and $f(X) \in O'[[X]]$ be any power series with $f \equiv \pi X \pmod{\deg 2}$ and $f \equiv X^q \pmod{p'}$.

THEOREM 2.1 (Relative Lubin–Tate group, [6, Chapter I, Theorem 1.3]). *There is a formal group $\mathcal{F}_f/O'$ such that*

$$\mathcal{F}_f^{\mathrm{Fr}} \circ f = f \circ \mathcal{F}_f.$$

When $k' = k$, this is Lubin and Tate's result, and in that case $\mathcal{F}_f$ is called the *Lubin–Tate group*.

Let W_f^i be the set of roots of $f^{(i)} := f^{\mathrm{Fr}^{i-1}} \circ \cdots \circ f(X)$, and a *primitive* element of W_f^i means an element of $W_f^i \backslash W_f^{i-1}$. Fix a primitive $\omega_i \in W^i_{f^{\mathrm{Fr}^{-i}}}$ such that $(\mathrm{Fr}^{-i} f)(\omega_i) = \omega_{i-1}$ for $1 \le i < \infty$ and let $k_i' = k'(\omega_i)$. (k_i' does not depend on the choice of ω_i.)

THEOREM 2.2 (Coleman, [6, Chapter I, Theorem 2.2]). *Let $\beta = (\beta_n)_{n=0}^{\infty}$ ($\beta_n \in k_n'$) be a norm-coherent sequence in the sense that $\beta_n \neq 0$ for every $n \ge 0$, and $N_{k_m/k_n}(\beta_m) = \beta_n$ for any m, n with $m \ge n \ge 0$. Let $v = v_{k_n'}(\beta_n)$. There is a unique $g_\beta \in X^v O'[[X]]^\times$ such that*

$$(\mathrm{Fr}^{-i} g_\beta)(\omega_i) = \beta_i \quad \text{for every } i \ge 1.$$

Thus, we can define the following for β as in Theorem 2.2.

DEFINITION 2.3 (Coates–Wiles derivative). Fix a logarithm $\lambda(X)$ of $\mathcal{F}_f$, and set

$$\delta_{n,\mathcal{F}_f}(\beta) := \left(\frac{d}{dX} \log g_\beta^{\mathrm{Fr}^{-n}}(X) \right) / \lambda'^{\mathrm{Fr}^{-n}}(X) \Big|_{X=\omega_n}$$

where $\lambda'(X)$ is the formal derivative of $\lambda(X)$.

For any $x_n \in \mathcal{F}_{f^{\mathrm{Fr}^n}}(k_n')$, there is $y_n \in \mathcal{F}_f(\overline{k'})$ with $f^{(n)}(y_n) = x_n$. Using the local Artin map, we define the pairing [6, p. 29]

$$(\,,\,)_n : \mathcal{F}_{f^{\mathrm{Fr}^n}}(k_n') \times k_n'^{\times} \to W_f^n, \qquad (x_n, u) \mapsto y_n^{[u,k_n']}[-]_{\mathcal{F}_f} y_n.$$

($[u, k_n']$ is the Artin symbol of u.)

For the following theorem, we assume $k' = k$.

THEOREM 2.4 (Explicit Reciprocity, [34]). *Let $\lambda(X)$ be a logarithm of $\mathcal{F}_f$. Let $\beta = (\beta_n) \in \varprojlim k_n^\times$. For any $x_n \in \mathcal{F}_f(k_n)$ we have*

$$(x_n, \beta_n)_n = \left[\frac{1}{\pi^n} \mathrm{Tr}_{k_n/k}(\lambda(x_n)\delta_{n,\mathcal{F}_f}(\beta)) \right](\omega_n).$$

(*The right-hand side does not depend on the choice of* λ. *Also note that we drop* n *from* $\delta_{n,\mathcal{F}_f}$ *because we assume* $k' = k$, *thus the action of* Fr *becomes irrelevant.*)

2.2. Plus/minus universal norms. Since this paper was written, much has been done in the area of Iwasawa theory for supersingular/non-ordinary reduction. Work similar to this section has also been done by Kitajima and Otsuki [15] in greater generality. In particular, they have done much to remove pesky conditions often attached to the "plus" points (like the condition $\varphi(p) \not\equiv p \pmod{p^2}$ in this paper). Their work cannot be immediately applied here because we deal with a formal group of a different Honda type, but their construction can be easily adapted with a slight modification. Since their work is already available, we will shorten our argument, and refer to that work when necessary.

Let k be the unramified quadratic extension $\mathbb{Q}_{p^2}$, and O be the ring of integers of k. Let $\rho \in k^\times$ be a uniformizer of k (i.e. $v_p(\rho) = 1$). Let ϕ be the pth Frobenius map, i.e., the non-trivial element of $\mathrm{Gal}(k/\mathbb{Q}_p)$. We let $k_\infty := k(\mu_{p^\infty})$ and let k'_∞ be the subextension of k_∞ such that $\mathrm{Gal}(k'_\infty/k) \cong \mathbb{Z}_p$. Let $k_n := k(\mu_{p^n})$ and k'_n be the subfield of k'_∞ such that $\mathrm{Gal}(k'_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$. (Thus $k'_n = k'^{\mathrm{Gal}(k_\infty/k'_\infty)}_{n+1}$.)

Let

$$l(X) := X + \frac{(1+X)^{p^2}-1}{\rho} + \frac{(1+X)^{p^4}-1}{\rho^2} + \cdots \in k[[X]].$$

It is easy to check that $l(X) = \sum_{n=1}^{\infty} a_n X^n$ with $na_n \in O$.

It is easy to check that

$$l^{\phi^2}(X^{p^2}) = \rho l(X) \pmod{pO[[X]]}.$$

Similar to [15, Section 3.1], by [10, Section 2, Theorem 2], there is a formal group F_ρ over O with $\log_{F_\rho}(X) = l(X)$ and Honda type $t^2 - \rho$.

PROPOSITION 2.5. *F_ρ is a Lubin–Tate group of height* 2 *and parameter* ρ.

Proof. A standard argument for formal groups. ∎

Also, by a standard argument, we have $\theta(X) = [\rho](X)$ where $[\rho](X)$ is the endomorphism of the Lubin–Tate group F_ρ with $[\rho](X) = \rho X + \cdots$. Hence

$$l([\rho](X)) = l(\exp_{F_\rho}(\rho l(X))) = \rho l(X),$$

and

$$l([\rho/p](X)) = \frac{\rho}{p} l(X). \tag{2.1}$$

Since F_ρ is a Lubin–Tate group of height 2 defined over O, similar to [16, Proposition 8.7] we can show the following:

PROPOSITION 2.6. *$F_\rho(k_\infty)$ is torsion-free.*

We choose $\epsilon \in F_\rho(k)$ to be an element such that

$$l(\epsilon) = -\rho - \rho^2 - \rho^3 - \cdots = -\frac{\rho}{1-\rho}.$$

REMARK 2.7. The construction of $l(x)$ and ϵ is similar to that of [15].

The first author and Bo-Hae Im's forthcoming paper [11], in which they try to establish Iwasawa theory for abelian varieties defined over totally ramified extensions, will shed more light on the reason why F_ρ and ϵ are defined as above.

Fix a primitive p^nth root ζ_{p^n} such that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for every $n \geq 1$. We define $b_n \in F_\rho(k_n)$ by

$$b_n := \epsilon[+]_{F_\rho}(\zeta_{p^n} - 1), \quad n \geq 0.$$

It is easy to check $\mathrm{Tr}_{k_n/k_{n-1}} l(b_n) = (p/\rho) l(b_{n-2})$ for every $n \geq 2$, and by (2.1),

$$l(\mathrm{Tr}_{k_n/k_{n-1}}[\rho/p](b_n)) = l(b_{n-2}).$$

Since $F_\rho(k_n)$ is torsion-free for any n, this implies

$$\mathrm{Tr}_{k_n/k_{n-1}}[\rho/p](b_n) = b_{n-2}.$$

Let $c_n := [\rho/p]^{[n/2]}(b_n)$. Then

$$\mathrm{Tr}_{k_n/k_{n-1}} c_n = c_{n-2} \quad \text{for every } n \geq 2.$$

Let $\tau_n(\chi) := \sum_{\sigma \in \mathrm{Gal}(k_n/k)} \chi(\sigma)\zeta_{p^n}^\sigma$ for a character χ of a subgroup of $\mathrm{Gal}(k_n/k)$. (In other words, in the definition of $\tau_n(\chi)$, χ is always considered to be a character of $\mathrm{Gal}(k_n/k)$.) We have the following simple proposition.

PROPOSITION 2.8. *Let χ be a primitive character of $\mathrm{Gal}(k_n/k)$. Then*

$$\sum_\sigma \chi(\sigma) l(c_n^\sigma) = (\rho/p)^{[n/2]} \tau_n(\chi).$$

Define

$$d_n := \mathrm{Tr}_{k_\infty/k'_\infty} c_{n+1}, \quad n \geq -1.$$

PROPOSITION 2.9. *Let χ be a primitive character of $\mathrm{Gal}(k'_n/k)$. Then*

$$\sum_{\sigma \in \mathrm{Gal}(k'_n/k)} \chi(\sigma) l(d_n^\sigma) = (\rho/p)^{[(n+1)/2]} \tau_{n+1}(\chi).$$

Proof. We have

$$\begin{aligned}\sum_{\sigma \in \mathrm{Gal}(k'_n/k)} \chi(\sigma) l(d_n^\sigma) &= \sum \chi(\sigma) l(\mathrm{Tr}_{k_{n+1}/k'_n} c_{n+1}^\sigma) \\ &= \sum_{\sigma \in \mathrm{Gal}(k_{n+1}/k)} \chi(\sigma) l(c_{n+1}^\sigma). \ \blacksquare\end{aligned}$$

Finally, we define the plus/minus universal norms as follows.

DEFINITION 2.10 (The plus/minus universal norms). For $n \geq 0$, we set

$$d_{2n}^{+} := d_{2n}, \quad d_{2n+1}^{+} := d_{2n}, \quad d_{2n-1}^{-} := d_{2n-1}, \quad d_{2n}^{-} := d_{2n-1}.$$

In particular, we have

$$l(d_{-1}^{-}) = -\frac{(p-1)\rho}{1-\rho}, \quad l(d_0^{+}) = \frac{\rho - p}{1-\rho},$$

which implies that d_{-1}^{-} generates $F_\rho(k)$ over O, and so does d_0^{+} if $\rho \not\equiv p \pmod{p^2}$ (hence our assumption $\varphi(p) \not\equiv p \pmod{p^2}$ for the plus Selmer group; more on this condition after Proposition 2.12).

Obviously, these points satisfy

$$\mathrm{Tr}_{k'_{2n}/k'_{2n-1}} d_{2n}^{+} = d_{2n-2}^{+}, \quad n \geq 1,$$
$$\mathrm{Tr}_{k'_{2n+1}/k'_{2n}} d_{2n+1}^{-} = d_{2n-1}^{-}, \quad n \geq 0$$

(hence the name).

DEFINITION 2.11 (The plus/minus norm subgroups). Let $k'_{-1} = k$. We define

$$F_\rho^{-}(k'_{-1}) := F_\rho(k'_{-1}), \quad F_\rho^{+}(k'_0) := F_\rho(k'_0),$$

and inductively, for $n \geq 0$,

$$F_\rho^{-}(k'_{2n+1}) := \{x \in F_\rho(k'_{2n+1}) \mid \mathrm{Tr}_{k'_{2n+1}/k'_{2n}} x \in F_\rho^{-}(k'_{2n-1})\},$$
$$F_\rho^{+}(k'_{2n+2}) := \{x \in F_\rho(k'_{2n+2}) \mid \mathrm{Tr}_{k'_{2n+2}/k'_{2n+1}} x \in F_\rho^{+}(k'_{2n})\}.$$

We let

$$\omega_n(X) := (1+X)^{p^n} - 1,$$
$$\omega_n^{+}(X) := X \prod_{2 \leq m \leq n,\, m \text{ even}} \omega_m(X)/\omega_{m-1}(X),$$
$$\omega_n^{-}(X) := X \prod_{1 \leq m \leq n,\, m \text{ odd}} \omega_m(X)/\omega_{m-1}(X),$$
$$\tilde{\omega}_n^{\pm}(X) := \omega_n(X)/\omega_n^{\mp}(X).$$

Let $G_n := \mathrm{Gal}(k'_n/k)$. We can identify $\mathbb{Z}_p[[G_\infty]]$ with $\Lambda = \mathbb{Z}_p[[X]]$ and $\mathbb{Z}_p[G_n]$ with $\Lambda_n = \mathbb{Z}_p[X]/(\omega_n(X))$ by identifying some topological generator of G_∞ with $X+1$. There is an isomorphism

$$i_n^{\pm} : \tilde{\omega}_n^{\mp}\Lambda_n \to \Lambda_n/(\omega_n^{\pm})$$

given by $1/\tilde{\omega}_n^{\mp}$.

Let T be the Tate module of F_ρ, set $V := T \otimes \mathbb{Q}_p$, and assume $T \cong \mathrm{Hom}(T, \mathbb{Z}_p(1))$ as a G_k-representation.

Let

$$D_n^{\pm} := \big\{x \in F_\rho(k'_n) \;\big|\; \text{for some } i \geq 0, \\ p^i x \text{ is a } \mathbb{Z}_p\text{-linear combination of } \{d_n^{\pm\sigma}\}_{\sigma\in G_n}\big\}.$$

(This group, when tensored with O, contains $F_\rho(k'_n)$ and its index is finite.)

PROPOSITION 2.12. *We have*

$$\mathrm{Hom}(D_n^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \tilde{\omega}_n^{\mp}\Lambda_n,$$
$$F_\rho^{\pm}(k'_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = O[G_n](d_n^{\pm}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

(*assuming* $\rho \not\equiv p \pmod{p^2}$ *for the plus case*).

Proof. The readers should also see [14, Proposition 3.11] and [16, Proposition 8.12]. A similar idea will be repeated later.

There is a pairing induced from $T \cong \mathrm{Hom}(T, \mathbb{Z}_p(1))$ by

$$(\,,\,)_n : (F_\rho(k'_n) \subset) H^1(k'_n, T) \times H^1(k'_n, T) \xrightarrow{\text{cup product}} H^2(k'_n, \mathbb{Z}_p(1)) \xrightarrow{\text{inv}} \mathbb{Z}_p.$$

For $x \in H^1(k'_n, T)$ we define the *Perrin–Riou map*

$$P_{n,x} : H^1(k'_n, T) \to \Lambda_n, \qquad z \mapsto \sum_{\sigma\in G_n} (x^\sigma, z)_n \sigma.$$

Similar to [16, Proposition 8.19] we have $\mathrm{im}(P_{n,d_n^{\pm}}) \subset \tilde{\omega}_n^{\mp}\Lambda_n$. Combining with the isomorphism $i_n^{\pm} : \tilde{\omega}_n^{\mp}\Lambda_n \to \Lambda_n/(\omega_n^{\pm})$ we get the $\pm$-*Coleman map*

$$\mathrm{Col}_n^{\pm} = i_n^{\pm} \circ P_{n,d_n^{\pm}} : H^1(k'_n, T) \to \Lambda_n/(\omega_n^{\pm})$$

with the commutative diagram

$$\begin{array}{ccc} H^1(k'_{n+1}, T) & \longrightarrow & \Lambda_{n+1}/(\omega_{n+1}^{\pm}) \\ \Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow{\scriptstyle \mathrm{Proj}} \\ H^1(k'_n, T) & \longrightarrow & \Lambda_n/(\omega_n^{\pm}) \end{array}$$

(We can show the commutativity similar to [16, Lemma 8.15].)

Naturally we have an exact sequence

$$0 \to \ker \mathrm{Col}_n^{\pm} \to H^1(k'_n, T) \to \mathrm{Hom}(D_n^{\pm}, \mathbb{Z}_p). \tag{2.2}$$

By taking the Pontryagin dual (denoted by $\vee$) we obtain

$$0 \to D_n^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(k'_n, V/T) \to (\ker \mathrm{Col}_n^{\pm})^\vee \to 0.$$

[The injectivity of the first map follows from the definition of $D_n^{\pm}$ [14, Remark 3.4]. Also, $H^1(k'_n, V/T) \cong H^1(k'_n, T)^\vee$ is given by the non-degeneracy of the local Tate pairing $H^1(k'_n, V/T) \times H^1(k'_n, T) \to \mathbb{Q}_p/\mathbb{Z}_p$.] Two things follow from this short exact sequence. First, $\ker \mathrm{Col}_n^{\pm}$ is the exact annihilator of $D_n^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ with respect to the local Tate pairing. Thus

$$D_n^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (H^1(k'_n, T)/\ker \mathrm{Col}_n^{\pm})^\vee.$$

Second, the last map in (2.2) is surjective.

For $n = 0$, from the discussion before Definition 2.11 it follows that $D_0^{\pm} = \mathbb{Z}_p(d_0^{\pm})$. Combined with the surjectivity of the last map in (2.2), this implies $\mathrm{Col}_0^{\pm}$ is surjective. By the Nakayama lemma every $\mathrm{Col}_n^{\pm}$ is surjective. Thus our first claim follows.

The second claim follows simply by comparing the O-coranks. ∎

Remark 2.13. Kitajima and Otsuki [15, Proposition 3.4, Remark 3.5, Lemma 3.6] carefully analyzed d_0^+ (in their notation, $\mathrm{Tr}_{0/-1}(d_0)$), and discovered a way to remove conditions similar to $\varphi(p) \not\equiv p \pmod{p^2}$ in many cases. Since our formal group has a different Honda type, it is not immediately clear that similar work can be done, but we certainly hope so.

3. CM elliptic curves

3.1. Setup. Let K be an imaginary quadratic field. Let F be an abelian extension of K, and E be an elliptic curve over F with complex multiplication by K with $\mathrm{End}(E) = O_K$. (Probably $\mathrm{End}(E) = O_K$ is not an important condition.)

We consider the Artin symbol $[\mathfrak{a}, L] \in \mathrm{Gal}(L^{\mathrm{ab}}/L)$ for any ideal $\mathfrak{a} \subset O_L$. In particular, for an ideal $a \subset O_K$, we set $\sigma_a := [a, K] = [a, K^{\mathrm{ab}}/K]$.

For $\alpha \in O_K$, let $[\alpha]$ denote the endomorphism of E whose differential is α. By the main theorem of complex multiplication [26] there is a Hecke character ψ of F with values in K satisfying

$$u^{[A,F]} = [\psi(A)](u)$$

for any ideal $A \subset O_F$ prime to the conductor of ψ and for any torsion u of E whose order is prime to the norm of A.

We assume $F(E_{\mathrm{tor}})$ is an abelian extension of K, which is equivalent to the existence of a Hecke character φ of K of type $(1, 0)$ such that

$$\psi = \varphi \circ N_{F/K} \tag{3.1}$$

(see [26, Theorem 7.44]).

Let $\mathfrak{f}_\varphi$ denote the conductor of φ, and let $\mathfrak{f}$ be any ideal divisible by both $\mathrm{cond}(F/K)$ and $\mathfrak{f}_\varphi$. Fix a prime number p which is prime to $\mathfrak{f}$, inert over $K/\mathbb{Q}$ (thus E has supersingular reduction at the primes above p), splitting completely over F/K, and inert over $K(\mathfrak{f})/F$ (i.e. every prime of F above p is inert in $K(\mathfrak{f})$). (For example, this happens when $K(\mathfrak{f}) = F$ and $p \equiv 1 \pmod{\mathfrak{f}}$.)

We let $O_p := O_{K_p}$. Then we can identify $T_p(E)$ with O_p such that G_F acts on $T_p(E)$ through some character $\kappa : G_F \to O_p^\times$. Indeed, $\kappa([A, F]) = \psi(A)$ for an ideal $A \subset O_F$ prime to $p \cdot \mathrm{cond}(\psi)$.

Let F_∞ be the maximal $\mathbb{Z}_p^2$-extension of F in $K(\mathfrak{f}p^\infty)$, $\mathbb{Q}_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, $\mathbb{Q}_n$ the subfield of $\mathbb{Q}_\infty$ with $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$, and

let $F_{\mathrm{cyc}} = F\mathbb{Q}_\infty$, $F_n = F\mathbb{Q}_n$. For a ring R we let

$$\Lambda_R := R[[\mathrm{Gal}(F_{\mathrm{cyc}}/F)]], \quad \Lambda_{R,n} := R[\mathrm{Gal}(F_n/F)],$$
$$\Lambda_R(K(\mathfrak{f}p^\infty)) := R[[\mathrm{Gal}(K(\mathfrak{f}p^\infty)/F)]].$$

We let M denote the maximal abelian p-extension of $K(\mathfrak{f}p^\infty)$ unramified outside the primes above p and let $X := \mathrm{Gal}(M/K(\mathfrak{f}p^\infty))$.

We fix an embedding $i : \bar{\mathbb{Q}} \to \mathbb{C}_p$; then complex conjugation induces a conjugation ϕ on $\mathbb{C}_p$. Note that ϕ restricted on K_p is the pth Frobenius map.

The embedding i fixes the prime q of F above p and the prime q_n of F_n, $q_{K(\mathfrak{f}p^n)}$ of $K(\mathfrak{f}p^n)$, q_{cyc} of F_{cyc}, q_∞ of F_∞, and $q_{K(\mathfrak{f}p^\infty)}$ of $K(\mathfrak{f}p^\infty)$ above q. For any ideal $a \subset O_K$ prime to $p \cdot \mathfrak{f}$, let F_a, $F_{n,a}$, $K(\mathfrak{f}p^n)_a$, $F_{\mathrm{cyc},a}$, $F_{\infty,a}$, and $K(\mathfrak{f}p^\infty)_a$ denote $F_{q^{\sigma_a}}$, $F_{n,q_n^{\sigma_a}}$, etc., so that we do not overload the notation.

Let $E^a := E^{\sigma_a}$ and $\hat{E}^a$ be the formal group over O_{F_a} associated to E^a.

3.2. The theory of complex multiplication. We fix a Weierstrass model for E,

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in F,$$

and write $\omega = dx/y$ for the corresponding differential of the first kind.

For the period lattice L of ω, the analytic uniformization of E is given by

$$\xi(\cdot, L) : \mathbb{C}/L \to E(\mathbb{C}), \quad \xi(z, L) = (\wp(z, L), \wp'(z, L)),$$

for the Weierstrass $\wp$-function $\wp(z, L)$ associated to the Weierstrass model.

Note that under our hypothesis, E is F-isogenous to E^σ for any Galois map $\sigma \in \mathrm{Gal}(\bar{K}/K)$. The main theorem of complex multiplication [26, 5.3] states that for any integral ideal $a \subset O_K$ prime to f_φ and to $\mathrm{cond}(F/K)$, there is a unique isogeny

$$\lambda(a) : E \to E^{\sigma_a}$$

over F of degree Na such that we have the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\nu(a)} & \mathbb{C}/L_a \\ {\scriptstyle \xi(\cdot,L)}\downarrow & & \downarrow{\scriptstyle \xi(\cdot,L_a)} \\ E(\mathbb{C}) & \xrightarrow{\lambda(a)} & E^{\sigma_a}(\mathbb{C}) \end{array}$$

for some $\nu(a) \in F$ and $L_a = \nu(a)a^{-1}L$. We also have

$$\sigma_a(u) = \lambda(a)(u)$$

for any $u \in E[c]$ with $(c, a) = 1$. We can check that ν satisfies the cocycle condition $\nu(ab) = \nu(a)^{\sigma_b}\nu(b)$, so we can extend ν to fractional ideals.

In addition, we can easily check that if $[a, F/K] = 1$, then $\nu(a) = \varphi(a)$.

3.3. Decomposition of Tate modules, plus/minus norm groups, etc. Let K' be the finite extension $K(\varphi, \bar{\varphi})$. Let K'_p be the topological closure of the image of K' under the embedding $i : \bar{\mathbb{Q}} \to \mathbb{C}_p$ fixed in Section 3.1. We let $R_p = O_{K'_p}[\mu_d]$ where $d = [F : K]$. Fix a set S of ideals of O_K such that $\{\sigma_a|_F\}_{a\in S} = \mathrm{Gal}(F/K)$.

We recall from Section 3.1 that we can identify T_p with O_p through the character $\kappa : G_F \to O_p^\times$. We let $\mathbf{T}$ and $\overline{\mathbf{T}}$ denote $T_p \otimes_{O_p} R_p$ and $T_p \otimes_{O_p,\phi} R_p$ (both free R_p-modules of rank 1). In both, R_p acts on the right, and in the latter the tensor is twisted by ϕ. In other words, $\overline{\mathbf{T}}$ is $T_p \otimes_{O_p} R_p$ on which G_F acts through $G_F \xrightarrow{\kappa} O_p^\times \xrightarrow{\phi} O_p^\times$. We check the following.

Proposition 3.1. *We have*

$$T_p \otimes_{\mathbb{Z}_p} R_p \cong \mathbf{T} \oplus \overline{\mathbf{T}}$$

and there are non-degenerate Galois-equivariant pairings

$$\mathbf{T} \times \overline{\mathbf{T}} \to R_p(1), \quad \overline{\mathbf{T}} \times \mathbf{T} \to R_p(1)$$

induced from the Weil pairing $T_p \times T_p \to \mathbb{Z}_p(1)$.

Proof. To prove the first claim, we let $O_p = \mathbb{Z}_p[\sqrt{D}]$ for some $D \in \mathbb{Z}_p^\times$. For any $\alpha \in O_p$, we let v_α be the corresponding element of T_p under the identification $T_p = O_p$. Let

$$w_1 = v_1 + \frac{1}{\sqrt{D}} v_{\sqrt{D}} = v_1 \otimes 1 + v_{\sqrt{D}} \otimes \frac{1}{\sqrt{D}} \in T_p \otimes R_p,$$
$$w_2 = v_1 - \frac{1}{\sqrt{D}} v_{\sqrt{D}} \in T_p \otimes R_p.$$

It is easy to show w_1 and w_2 generate $T \otimes R_p$ over R_p and $R_p(w_1) \cong \mathbf{T}$ and $R_p(w_2) \cong \overline{\mathbf{T}}$.

The Weil pairing induces a pairing $\mathbf{T} \oplus \overline{\mathbf{T}} \times \mathbf{T} \oplus \overline{\mathbf{T}} \to R_p(1)$. The second claim follows easily. The only non-obvious point is that it induces a pairing $\mathbf{T} \times \overline{\mathbf{T}}$ rather than $\mathbf{T} \times \mathbf{T}$, which we can check by looking at the action of G_F on $\mathbf{T}$, $\overline{\mathbf{T}}$, and $R_p(1)$. ∎

The cup product and the invariant map induce

$$(\ ,\ )_n : H^1(F_{n,a}, \mathbf{T}) \times H^1(F_{n,a}, \overline{\mathbf{T}}) \to H^2(F_{n,a}, R_p(1)) \xrightarrow{\mathrm{inv}} R_p,$$

which in turn induces

$$(\ ,\ )_n : \hat{E}^a(F_{n,a}) \otimes_{O_p} R_p \times H^1(F_{n,a}, \overline{\mathbf{T}}) \to R_p.$$

Similarly $\overline{\mathbf{T}} \times \mathbf{T} \to R_p(1)$ induces

$$(\ ,\ )_n : \hat{E}^a(F_{n,a}) \otimes_{O_p,\phi} R_p \times H^1(F_{n,a}, \mathbf{T}) \to R_p.$$

For $x = (x_{n,a}) \in \prod_{a\in S} \hat{E}^a(F_{n,a}) \otimes_{O_p} R_p$ we define the Perrin–Riou map

$$P_{n,x} : \prod_{a\in S} H^1(F_{n,a}, \overline{\mathbf{T}}) \to \Lambda_{R_p,n}, \qquad (z_a) \mapsto \sum_{a\in S} \sum_{\sigma\in G_n} (x_{n,a}^\sigma, z_a)_n \sigma.$$

Recall the Lubin–Tate group F_ρ over O_p of height 2 and parameter $\rho = \varphi(p)$ defined in Section 2.2. We note that $\hat{E}^a$ is a Lubin–Tate group over $O_{F_a} = O_p$ of height 2 and of parameter $\nu(p) = \varphi(p)$ [6, p. 46]. We also note that all the Lubin–Tate groups of the same height and parameter are isomorphic, so $\hat{E}^a$ is O_p-isomorphic to F_ρ.

We fix an isomorphism $i_a : F_\rho \to \hat{E}^a$ such that $\log_{\hat{E}^a} \circ i_a = \log_{F_\rho}$.

Definition 3.2. Since $\mathrm{Gal}(F_{\mathrm{cyc}}/K) = \mathrm{Gal}(F/K) \times \mathrm{Gal}(F_{\mathrm{cyc}}/F)$, we can write any $\sigma \in \mathrm{Gal}(F_{\mathrm{cyc}}/K)$ as $(\tilde{\sigma}, \sigma')$ for unique $\tilde{\sigma} \in \mathrm{Gal}(F/K)$ and $\sigma' \in \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Recall the plus/minus universal norms $d_n^\pm \in F_\rho^\pm(F_{n,a})$ of Section 2.2. We let $d_{n,a}^\pm \in \hat{E}^{a,\pm}(F_{n,a})$ be $i_a(d_n^\pm)$. For a character η of $\mathrm{Gal}(F/K)$, we let

$$d_{n,\eta}^\pm := \sum_{a\in S} \frac{\nu(a)}{\varphi(a)} \eta(\sigma_a|_F) d_{n,a}^{\pm,\sigma'_a} \in \bigoplus_{a\in S} \hat{E}^{a,\pm}(F_{n,a}) \otimes_{O_p} R_p,$$

$$\bar{d}_{n,\eta}^\pm := \sum_{a\in S} \left(\frac{\nu(a)}{\varphi(a)}\right)^\phi \eta(\sigma_a|_F) d_{n,a}^{\pm,\sigma'_a} \in \bigoplus_{a\in S} \hat{E}^{a,\pm}(F_{n,a}) \otimes_{O_p,\phi} R_p$$

where $\sigma'_a = (\sigma_a|_{F_{\mathrm{cyc}}})'$.

Proposition 3.3. (*For the plus part, assume* $\varphi(p) \not\equiv p \pmod{p^2}$.) *Let* $D_p = \mathrm{Frac}(R_p)/R_p$. *For each character* η *of* $\mathrm{Gal}(F/K)$ *there is* $f_\eta^\pm$ *such that* $\mathrm{Hom}(\bigoplus_{a\in S} \hat{E}^{a,\pm}(F_{\infty,a}) \otimes_{O_p} D_p, D_p)$ *is* Λ_{R_p}*-free of rank* d *generated by* $\{f_\eta^\pm\}_\eta$, *and for every character* $\chi : \mathrm{Gal}(F_n/F) \to \mu_{p^n}$,

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)} \chi(\sigma) f_\eta^\pm(d_{n,\eta}^{\pm\sigma} \otimes p^{-k}) = \chi(\tilde{\omega}_n^{\mp}) p^{-k}.$$

Similarly, there is $\bar{f}_\eta^\pm$ *such that* $\mathrm{Hom}(\bigoplus_{a\in S} \hat{E}^{a,\pm}(F_{\infty,a}) \otimes_{O_p,\phi} D_p, D_p)$ *is* Λ_{R_p}*-free of rank* d *generated by* $\{\bar{f}_\eta^\pm\}_\eta$, *and for every character* $\chi : \mathrm{Gal}(F_n/F) \to \mu_{p^n}$,

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)} \chi(\sigma) \bar{f}_\eta^\pm(\bar{d}_{n,\eta}^{\pm\sigma} \otimes p^{-k}) = \chi(\tilde{\omega}_n^{\mp}) p^{-k}.$$

Proof. Let $D_{n,\eta}^\pm := R_p[G_n] d_{n,\eta}^\pm$. Let $P_{n,\eta}^\pm = P_{n,d_{n,\eta}^\pm}$ be the Perrin–Riou map mentioned before Definition 3.2, and define $\mathrm{Col}_{n,\eta}^\pm$ as in the proof of Proposition 2.12. Since $\{d_{0,\eta}^\pm\}_\eta$ generates $\prod_{a\in S} \hat{E}^a(F_{0,a}) \otimes R_p$, again each $\mathrm{Col}_{n,\eta}^\pm$ is surjective (onto $\Lambda_{R_p,n}/(\omega_n^\pm)$).

Similar to the proof of Proposition 2.12 we have

$$\prod_a H^1(F_{n,a}, \overline{\mathbf{T}})/\ker(\mathrm{Col}_{n,\eta}^\pm) \cong \mathrm{Hom}(D_{n,\eta}^\pm \otimes \mathbb{Q}_p/\mathbb{Z}_p, D_p)$$

and a commutative diagram

$$\begin{array}{ccc}\mathrm{Hom}(D^{\pm}_{m,\eta}, R_p) \cong \mathrm{Hom}(D^{\pm}_{m,\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p, D_p) & \xrightarrow{\sim} & \tilde{\omega}_m^{\mp} \Lambda_{R_p,m} \\ \downarrow & & \downarrow \\ \mathrm{Hom}(D^{\pm}_{n,\eta}, R_p) \cong \mathrm{Hom}(D^{\pm}_{n,\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p, D_p) & \xrightarrow{\sim} & \tilde{\omega}_n^{\mp} \Lambda_{R_p,n}\end{array}$$

where the horizontal maps are the Perrin–Riou maps instead of $\pm$-Coleman maps, the left vertical map is restriction and the right one sends $\tilde{\omega}_m^{\mp}$ to $\tilde{\omega}_n^{\mp}$.

Now we choose the generator $f_\eta^{\pm}$ of

$$\mathrm{Hom}(D^{\pm}_{\infty,\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p, D_p) = \varprojlim \mathrm{Hom}(D^{\pm}_{n,\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p, D_p)$$

that maps to $\tilde{\omega}_n^{\mp}$ for each n. Note that $\bigoplus_\eta D^{\pm}_{\infty,\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p = \bigoplus_{a \in S} \hat{E}^{a,\pm}(F_{\infty,a}) \otimes_{O_p} D_p$. This $f_\eta^{\pm}$ has the prescribed property.

Finding $\bar{f}_\eta^{\pm}$ is similar. ∎

3.4. Elliptic units. By replacing E with E^σ for some $\sigma \in G_K$, we can assume the period lattice L of E is given by $L = \Omega_E \mathfrak{f}$ for some $\Omega_E \in \mathbb{C}^\times$.

Recall ξ, λ and ν from Section 3.2. Let Fr be the p^2th Frobenius map. For every $n \geq 0$ there is an $\mathfrak{f}$-division point w_n of $p^n L$ such that

$$\mathrm{Fr}^n \, \xi\big(\nu(p^{-n}) w_n, \nu(p^{-n}) p^n L\big) = \xi(\Omega_E, L).$$

It follows that $w_0 \equiv \Omega_E \pmod{L}$ and $w_n \equiv w_{n-1} \pmod{p^{n-1}L}$ for $n \geq 1$. Then there exists $u_n \in L/p^n L$ for every $n \geq 0$ satisfying

$$w_n - u_n = \Omega_E \pmod{p^n L}.$$

It follows that $u_n \equiv u_{n-1} \pmod{p^{n-1}L}$ for $n \geq 1$. Let $L_{-n} := \nu(p^{-n}) p^n L$. By the main theorem of complex multiplication we have

$$\lambda(p)\big(\xi(\nu(p^{-n}) u_n, L_{-n})\big) = \xi\big(\nu(p^{-n+1}) u_{n-1}, L_{-n+1}\big).$$

We consider

$$\pi_n^a = \xi\big(\nu(a)\nu(p^{-n}) u_n, \nu(a) a^{-1} L_{-n}\big) \in E(K(\mathfrak{f}p^n))$$

as a local point of $E^a(K(\mathfrak{f}p^n)_a)$. Since it is a p^n-torsion point and E^a has supersingular reduction at q^{σ_a}, we can consider it as a point in the formal completion $\hat{E}^a(K(\mathfrak{f}p^n)_a)$.

Definition 3.4. Let I denote the set of integral ideals of K prime to $6\mathfrak{f}p$. For $b \in I$ we define

$$\Theta(z, L; b) := \prod_\lambda (\wp(z, L) - \wp(\lambda, L))^{-6} \triangle(L)^{Na} / \triangle(a^{-1} L)$$

where $\triangle$ is the discriminant function and λ runs over the non-zero residue classes of $b^{-1}L/L$.

We define the elliptic unit

$$\xi_{n,b} := \Theta(\nu(p^{-n}) \Omega_E, L_{-n}; b).$$

Also we define its inverse limit $\xi_b = (\xi_{n,b})$ with respect to the norm $N_{K(\mathfrak{f}p^{n+1})/K(\mathfrak{f}p^n)}$.

Note that $\xi_{n,b}^{\sigma_a} = \Theta(\nu(a)\nu(p^{-n})\Omega_E, \nu(a)a^{-1}L_{-n}; b)$ for any $a \in I$. Here $\pi_n^a \in \hat{E}^a(F_{n,a})$ satisfies $\hat{\lambda}(p)(\pi_n^a) = \pi_{n-1}^a$.

Recall the definition of Coates–Wiles derivative (Definition 2.3). Define

$$P_a(z) := \Theta(\nu(a)\Omega_E - z, \nu(a)a^{-1}L; b) \quad \text{(as a power series)},$$
$$Q_a(X) := P_a(\lambda_{\hat{E}^a}(X)).$$

By [5, Lemma 23] or [6, Chapter 2, p. 72], $Q_a(X) \in O_{K(\mathfrak{f})_a}[[X]]$. Similar to [5], [22, Section 6], or [6, Chapter 2, Section 4.9], we can show $Q_a^{\mathrm{Fr}^{-n}}(\pi_n^a) = \Theta(\nu(a)\nu(p^{-n})\Omega_E, \nu(a)a^{-1}L_{-n}; b) = \xi_{n,b}^{\sigma_a}$. Thus $g_{\xi_b^{\sigma_a}}(X) = Q_a(X)$, and we have the following.

PROPOSITION 3.5. *Let $\delta_{n,a}(u)$ denote the Coates–Wiles derivative $\delta_{n,\hat{E}^a}(u)$ with respect to π_n^a. Then*

$$\delta_{n,a}(\xi_b^{\sigma_a}) = -12\frac{\varphi(a)}{\nu(a)}\frac{\varphi(p)^n}{\Omega_E}\left[NbL_{\mathfrak{f}p^n}(\bar{\varphi}, \sigma_a, 1) - \varphi(b)L_{\mathfrak{f}p^n}(\bar{\varphi}, \sigma_{ab}, 1)\right]$$

where $L_{\mathfrak{f}p^n}(\bar{\varphi}, \sigma_a, s)$ is $\sum_c \bar{\varphi}(c)/(Nc)^s$ with c running over the integral ideals of K with $[c, K(\mathfrak{f}p^n)/K] = \sigma_a|_{K(\mathfrak{f}p^n)}$.

Proof. By definition we have

$$\begin{aligned}\delta_{n,a}(\xi_b^{\sigma_a}) &= \frac{d}{dz}\log P_a^{\mathrm{Fr}^{-n}}(z)\Big|_{z=\nu(a)\nu(p^{-n})u_n} \\ &= \frac{d}{dz}\log\Theta\big(\nu(a)\nu(p^{-n})w_n - z, \nu(a)a^{-1}L_{-n}; b\big)\Big|_{z=\nu(a)\nu(p^{-n})u_n} \\ &= \frac{d}{dz}\log\Theta\big(\nu(a)\nu(p^{-n})\Omega_E - z, \nu(a)a^{-1}L_{-n}; b\big)\Big|_{z=0}.\end{aligned}$$

By [22, Proposition 6.7] or [6, p. 62], we obtain our claim. ∎

PROPOSITION 3.6. *Let c and d be any ideals in I and assume $[d, F/K] = 1$. Then*

$$\left(\frac{\varphi(c)}{\nu(c)}\frac{L_{\mathfrak{f}p^n}(\bar{\varphi}, \sigma_c, 1)}{\Omega_E}\right)^{\sigma_d} = \frac{\varphi(cd)}{\nu(cd)}\frac{L_{\mathfrak{f}p^n}(\bar{\varphi}, \sigma_{cd}, 1)}{\Omega_E}.$$

Proof. Combine [6, Chapter 2, Propositions 3.3 and 3.5]. ∎

3.5. Kummer pairing and explicit reciprocity law

DEFINITION 3.7. For an extension L of $\mathbb{Q}_p$, let U_L denote the pro-p-part of the units $O_L^\times$. Let $U_{K(\mathfrak{f}p^n)} := \bigoplus_{a\in S} U_{K(\mathfrak{f}p^n)_a}$, $\mathcal{U}_a := \varprojlim U_{K(\mathfrak{f}p^n)_a}$, and $\mathcal{U} := \bigoplus_{a\in S}\mathcal{U}_a$. (The inverse limit is with respect to the norm.)

Let $\mathcal{E}_{K(\mathfrak{f}p^n)}$ denote the closure of the projection of the global units $O_{K(\mathfrak{f}p^n)}^\times$ into $U_{K(\mathfrak{f}p^n)}$, and let $\mathcal{E} := \varprojlim \mathcal{E}_{K(fp^n)}$.

Let $\mathcal{C}$ denote the closure in $\mathcal{E}$ of the group generated over $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ by the elliptic units ξ_b as b runs over integral ideals of K prime to $6\mathfrak{f}p$.

Recall the definition of M in Section 3.1 and $X = \mathrm{Gal}(M/K(\mathfrak{f}p^\infty))$.

We make the following notation.

Definition 3.8. Recall we can identify T with O_p so $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/F)$ acts on T as multiplication by the character $\kappa : \mathrm{Gal}(K(\mathfrak{f}p^\infty)/F) \to O_p^\times$.

For any $\mathbb{Z}_p$-module M with $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/F)$ action on it, we define Λ_{R_p}-modules

$$M^{\kappa}_{F_{\mathrm{cyc}}} := M \otimes R_p(\kappa^{-1}) \otimes_{\Lambda_{R_p}(K(\mathfrak{f}p^\infty))} \Lambda_{R_p},$$
$$M^{\bar\kappa}_{F_{\mathrm{cyc}}} := M \otimes R_p(\bar\kappa^{-1}) \otimes_{\Lambda_{R_p}(K(\mathfrak{f}p^\infty))} \Lambda_{R_p}$$

where $\bar\kappa$ denotes $\phi \circ \kappa$.

We consider ξ_b as an element embedded in $\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}}$ and $\mathcal{C}^{\bar\kappa}_{F_{\mathrm{cyc}}}$.

Proposition 3.9. *Let $b = (x_b)$ be a principal prime of K generated by $x_b \in O_K$ prime to $6\mathfrak{f}p$ with $[b, F/K] = 1$, and assume that $\varphi(b) - Nb \not\equiv 0 \pmod p$ and $\bar\varphi(b) - Nb \not\equiv 0 \pmod p$. Then ξ_b generates $\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}}$ and $\mathcal{C}^{\bar\kappa}_{F_{\mathrm{cyc}}}$ over $R_p[[\mathrm{Gal}(F_{\mathrm{cyc}}/K)]]$.*

Proof. The proof is the same as that of [23, Proposition 11.6]. ∎

Note that the condition in Proposition 3.9 implies that b splits completely over F/K. Once and for all, we fix $b = (x_b)$ that splits completely in $K(\mathfrak{f})/K$ such that $x_b \not\equiv 0, 1 \pmod p$.

We let $\mathcal{U}^{\kappa}_{\mathrm{cyc},a}$ and $\mathcal{U}^{\bar\kappa}_{\mathrm{cyc},a}$ denote $(\mathcal{U}_a)^{\kappa}_{F_{\mathrm{cyc}}}$ and $(\mathcal{U}_a)^{\bar\kappa}_{F_{\mathrm{cyc}}}$.

Definition 3.10. For a field L/F, the *Selmer group* of E over L is

$$\mathrm{Sel}_p(E/L) := \ker\left(H^1(L, E[p^\infty]) \to \prod_v \frac{H^1(L_v, E[p^\infty])}{E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v runs over all places.

We have

$$\mathrm{Sel}_p(E/K(\mathfrak{f}p^\infty)) \cong \mathrm{Hom}(X, E[p^\infty])$$

for $X = \mathrm{Gal}(M/K(\mathfrak{f}p^\infty))$ [6, 4.1, p. 124].

Let $D_p := \mathrm{Frac}(R_p)/R_p$, $\mathbf{A} := \mathbf{T} \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and $\bar{\mathbf{A}} := \overline{\mathbf{T}} \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We have

$$\begin{aligned}
\mathrm{Sel}_{R_p}(E/F_{\mathrm{cyc}}) &:= \mathrm{Sel}_p(E/F_{\mathrm{cyc}}) \otimes R_p \\
&\cong \mathrm{Hom}_{R_p}(X \otimes R_p, E[p^\infty] \otimes R_p)^{\mathrm{Gal}(K(\mathfrak{f}p^\infty)/F_{\mathrm{cyc}})} \\
&\cong \mathrm{Hom}_{R_p}(X \otimes R_p, \mathbf{A} \oplus \bar{\mathbf{A}})^{\mathrm{Gal}(K(\mathfrak{f}p^\infty)/F_{\mathrm{cyc}})} \\
&\cong \mathrm{Hom}_{R_p}(X^{\kappa}_{F_{\mathrm{cyc}}}, D_p) \oplus \mathrm{Hom}_{R_p}(X^{\bar\kappa}_{F_{\mathrm{cyc}}}, D_p).
\end{aligned}$$

On the other hand, for any $a \in S$,

$$\hat{E}(F_{\mathrm{cyc},a}) \otimes_{O_p} D_p \xrightarrow{\sim} H^1(F_{\mathrm{cyc},a}, \mathbf{A}),$$

(see Hazewinkel's series of papers on this subject or [4]). On the other hand, we have the following.

PROPOSITION 3.11.

$$H^1(F_{\mathrm{cyc},a}, \mathbf{A}) \cong \mathrm{Hom}(\mathcal{U}^{\kappa}_{\mathrm{cyc},a}, D_p).$$

Proof. We can prove this via the Hochschild–Serre spectral sequence and the long exact sequence of cohomology groups [24, Proposition 5.4]. ∎

It follows that $E(F_{\mathrm{cyc},a}) \otimes_{O_p} D_p \cong \mathrm{Hom}(\mathcal{U}^{\kappa}_{\mathrm{cyc},a}, D_p)$, and similarly $E(F_{\mathrm{cyc},a}) \otimes_{O_p,\phi} D_p \cong \mathrm{Hom}(\mathcal{U}^{\bar{\kappa}}_{\mathrm{cyc},a}, D_p)$.

We observe that these isomorphisms obviously come from the following Kummer pairings. Recall that π^a_n is a primitive root of $f^{(n)} := \hat{\lambda}(p)^{\mathrm{Fr}^{n-1}} \circ \cdots \circ \hat{\lambda}(p)$. For each $n > 0$, we have the Kummer pairing

$$\langle\,,\rangle_{K(\mathfrak{f}p^n)_a} : \hat{E}^a(K(\mathfrak{f}p^n)_a) \times U_{K(\mathfrak{f}p^n)_a} \to \hat{E}^a[\rho^n],$$
$$(x,u) \mapsto \langle x,u\rangle_{K(\mathfrak{f}p^n)_a} = \alpha_n^{[u,K(\mathfrak{f}p^n)_a]} - \alpha_n,$$

where α_n is any root of $f^{(n)}(X) = x$. This pairing does not depend on the choice of α_n. Since $\hat{E}^a[\rho^n] = O_p/\rho^n O_p \cdot \pi^a_n$, we can consider it as a pairing $\langle\,,\rangle_{K(\mathfrak{f}p^n)_a} : \hat{E}^a(K(\mathfrak{f}p^n)_a) \times U_{K(\mathfrak{f}p^n)_a} \to O_p/\rho^n O_p$. Then it is easy to check that if $N_{K(\mathfrak{f}p^{n+1})_a/K(\mathfrak{f}p^n)_a} u_{n+1} = u_n$, then $\langle x, u_{n+1}\rangle_{K(\mathfrak{f}p^{n+1})_a} \equiv \langle x, u_n\rangle_{K(\mathfrak{f}p^n)_a} \pmod{\rho^n}$ for any $x \in \hat{E}^a(K(\mathfrak{f}p^n)_a)$, and thus we have a pairing

$$\langle\,,\rangle_{K(\mathfrak{f}p^\infty)_a} : \hat{E}^a(K(\mathfrak{f}p^\infty)_a) \times U_a \to O_p.$$

Since $\langle\,,\rangle_{K(\mathfrak{f}p^\infty)_a}$ is O_p-linear on $\hat{E}^a(K(\mathfrak{f}p^\infty)_a)$, there is a pairing

$$\langle\,,\rangle_{K(\mathfrak{f}p^\infty)_a,\phi} : \hat{E}^a(K(\mathfrak{f}p^\infty)_a) \otimes_{O_p,\phi} O_p \times U_a \to O_p$$

given by $\langle x,u\rangle_{K(\mathfrak{f}p^\infty)_a,\phi} = \phi(\langle x,u\rangle_{K(\mathfrak{f}p^\infty)_a})$.

Similarly we can define

$$\langle\,,\rangle_a : \bigcup_n \hat{E}^a(F_a(\pi^a_n)) \times \varprojlim U_{F_a(\pi^a_n)} \to O_p,$$
$$\langle\,,\rangle_{a,\phi} : \bigcup_n \hat{E}^a(F_a(\pi^a_n)) \otimes_{O_p,\phi} O_p \times \varprojlim U_{F_a(\pi^a_n)} \to O_p.$$

Here we should note that $K(\mathfrak{f}p^n)_a = K(\mathfrak{f})_a F_a(\pi^a_n)$ and from now on we make the identifications $\mathrm{Gal}(K(\mathfrak{f}p^n)_a/F_a(\pi^a_n)) \cong \mathrm{Gal}(K(\mathfrak{f})_a/F_a)$ and $\mathrm{Gal}(K(\mathfrak{f})_a/F_a) \cong \mathrm{Gal}(K(\mathfrak{f})/F)$.

For notational convenience, we let ξ denote ξ_b for a fixed b, and identify ξ with its image in $\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}$ and $\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}$. Let χ be a character of $G'_n = \mathrm{Gal}(K(\mathfrak{f}p^n)_a/K(\mathfrak{f})_a) \cong \mathrm{Gal}(F_a(\pi^a_n)/F_a)$. For $u \in U_a$, define

$$\delta_{\chi,a}(u) := \frac{1}{|G'_n|} \sum_{\gamma \in G'_n} \chi(\gamma)\delta_{n,a}(u)^\gamma,$$

and for $x \in \hat{E}^a(K(\mathfrak{f}p^n)_a)$,

$$\lambda_{\chi,a}(x) := \frac{1}{|G'_n|} \sum_{\gamma \in G'_n} \chi^{-1}(\gamma) \lambda_{\hat{E}^a}(x)^\gamma.$$

Similar to [24, Proposition 5.6], explicit reciprocity (Theorem 2.4) yields the following: For $x \in \hat{E}^a(F_a(\pi_n^a))$, $u \in \varprojlim U_{F_a(\pi_n^a)}$, and $\sigma \in G'_n$,

$$\langle x^\sigma, u \rangle_a = \frac{1}{\rho^n} \sum_{\chi \in \hat{G}'_n} \chi(\sigma)(|G'_n|\delta_{\chi,a}(u)) \cdot \lambda_{\chi,a}(x).$$

Recall that $F_n = F\mathbb{Q}_n$. Suppose $x \in \hat{E}^a(F_{n-1,a})$. Then $\lambda_{\chi,a}(x) = 0$ if χ is not trivial on $\mathrm{Gal}(F_a(\pi_n^a)/F_{n-1,a})$, and thus

$$\langle x^\sigma, u \rangle_a = \frac{1}{\rho^n} \sum_{\chi \in \hat{G}_{n-1}} \chi(\sigma)|G'_n|\delta_{\chi,a}(u)\lambda_{\chi,a}(x)$$

where χ is considered a character of both $G_{n-1} := \mathrm{Gal}(F_{n-1,a}/F_a)$ and G'_n. Thus for a fixed $\chi \in \hat{G}_{n-1}$,

$$\Big\langle \sum_{\sigma' \in G_{n-1}} \chi^{-1}(\sigma') x^{\sigma\sigma'}, u \Big\rangle_a = \frac{1}{\rho^n} \chi(\sigma)(|G'_n|\delta_{\chi,a}(u))(|G_{n-1}|\lambda_{\chi,a}(x)).$$

We have the following proposition.

Proposition 3.12. *Let χ be a primitive character of G_n, η be a character of $\mathrm{Gal}(F/K)$, $d^{\pm}_{n,\eta}$ be the points defined in Section 3.3, and $\langle\,,\rangle$ and $\langle\,,\rangle_\phi$ be the pairings given by summing $\langle\,,\rangle_{K(fp^\infty)_a}$ and $\langle\,,\rangle_{K(fp^\infty)_a,\phi}$ over all $a \in S$. If $(-1)^n \equiv \epsilon$, then*

$$\sum_{\sigma \in G_n} \chi^{-1}(\sigma)\langle d^{\pm\sigma}_{n,\eta}, \xi\rangle = -12\left[Nb\frac{L(\bar{\varphi}, \eta\chi, 1)}{\Omega_E} - \varphi(b)\chi^{-1}(\sigma_b)\eta^{-1}(\sigma_b|_F)\frac{L(\bar{\varphi}, \eta\chi, 1)}{\Omega_E}\right] \times [\rho/p]^{[(n+1)/2]}\tau_{n+1}(\chi^{-1}),$$

and

$$\sum_{\sigma \in G_n} \chi^{-1}(\sigma)\langle \bar{d}^{\pm\sigma}_{n,\eta}, \xi\rangle_\phi = -12\left[Nb\frac{L(\varphi, \eta\chi, 1)}{\bar{\Omega}_E} - \bar{\varphi}(b)\chi^{-1}(\sigma_b)\eta^{-1}(\sigma_b|_F)\frac{L(\varphi, \eta\chi, 1)}{\bar{\Omega}_E}\right] \times [\bar{\rho}/p]^{[(n+1)/2]}\tau_{n+1}(\chi^{-1}).$$

Proof. Throughout the proof, we use the decomposition $\mathrm{Gal}(K(\mathfrak{f}p^n)_a/F_a) \cong \mathrm{Gal}(F_a(\pi_n^a)/F_a) \times \mathrm{Gal}(K(\mathfrak{f})_a/F_a)$ and the identification $\mathrm{Gal}(K(\mathfrak{f})_a/F_a) = \mathrm{Gal}(K(\mathfrak{f})/F)$. We note that the embedded image of ξ in $\mathcal{U}$ is $(\xi^{\sigma_a})_{a\in S}$. We

have

$$\Big\langle \sum_{\sigma\in G_n} \chi^{-1}(\sigma) d_{n,\eta}^{\pm,\sigma}, \xi \Big\rangle = \sum_{a\in S} \frac{\nu(a)}{\varphi(a)} \eta(\sigma_a) \Big\langle \sum \chi^{-1}(\sigma) d_{n,a}^{\pm,\sigma'_a\sigma}, \xi^{\sigma_a} \Big\rangle_{K(\mathfrak{f}p^\infty)_a}$$
$$= \sum_{a\in S} \frac{\nu(a)}{\varphi(a)} \eta(\sigma_a) \Big\langle \sum_{\sigma\in G_n} \chi^{-1}(\sigma) d_{n,a}^{\pm,\sigma'_a\sigma}, N\xi^{\sigma_a} \Big\rangle_a$$
$$= \sum_{a\in S} \frac{\nu(a)}{\varphi(a)} \eta(\sigma_a) \frac{1}{\rho^{n+1}} \chi(\sigma_a) (\big|G'_{n+1}\big| \, \delta_{\chi,a}(N\xi^{\sigma_a})) \cdot (|G_n| \lambda_{\chi,a}(d_{n,a}^{\pm})).$$

(Here N stands for the norm $N_{K(\mathfrak{f}p^\infty)_a/F_a(\pi_\infty^a)}$.)

We want to compute $\delta_{\chi,a}(N\xi^{\sigma_a})$. For any $\tau \in \mathrm{Gal}(K(\mathfrak{f}p^n)_a/F_a(\pi_n^a))$,

$$(g_{\xi^{\sigma_a}}^{\mathrm{Fr}^{-n}}(\pi_n^a))^\tau = (g_{\xi^{\sigma_a}}^\tau)^{\mathrm{Fr}^{-n}}(\pi_n^a)$$

where Fr is the p^2th Frobenius map that generates $\mathrm{Gal}(F_a^{\mathrm{un}}/F_a)$. Thus $g_{N\xi^{\sigma_a}} = \prod_{\tau\in\mathrm{Gal}(K(\mathfrak{f})_a/F_a)} g_{\xi^{\sigma_a}}^\tau$. By Propositions 3.5 and 3.6 we have

$$\delta_{n+1,a}(N\xi^{\sigma_a}) = \frac{\sum_{\tau\in\mathrm{Gal}(K(\mathfrak{f})_a/F_a)} d\log g_{\xi^{\sigma_a}}^{\tau\,\mathrm{Fr}^{-n-1}}(X)/dX}{\lambda'_{\hat{E}^a}{}^{\mathrm{Fr}^{-n-1}}(X)}\Big|_{X=\pi_{n+1}^a}$$
$$= \sum_{\tau\in\mathrm{Gal}(K(\mathfrak{f})_a/F_a)} \left(\frac{d\log g_{\xi^{\sigma_a}}^{\mathrm{Fr}^{-n-1}}(X)/dX}{\lambda'_{\hat{E}^a}{}^{\mathrm{Fr}^{-n-1}}(X)}\Big|_{X=\pi_{n+1}^a} \right)^\tau$$
$$= \sum_{\tau\in\mathrm{Gal}(K(\mathfrak{f})/F)} \delta_{n+1,a}(\xi^{\sigma_a})^\tau$$
$$= \sum_{\tau\in\mathrm{Gal}(K(\mathfrak{f})/F)} -12\frac{\varphi(a)}{\nu(a)}\varphi(p)^{n+1} \times \left[Nb \frac{L_{\mathfrak{f}p^{n+1}}(\bar{\varphi}, \sigma_a\tau, 1)}{\Omega_E} - \varphi(b) \frac{L_{\mathfrak{f}p^{n+1}}(\bar{\varphi}, \sigma_{ab}\tau, 1)}{\Omega_E} \right].$$

Since $|G_n|\lambda_{\chi,a}(d_{n,a}^{\pm}) = \sum_{\sigma\in G_n} \lambda_{\hat{E}^a}(d_{n,a}^{\pm})^\sigma = (\rho/p)^{[(n+1)/2]}\tau_{n+1}(\chi^{-1})$ (Proposition 2.9), the first claim follows (again) by Proposition 3.6.

The second statement follows similarly. We only need to observe that $\overline{\tau_{n+1}(\chi)} = \chi(-1)\tau_{n+1}(\bar{\chi}) = \tau_{n+1}(\chi^{-1})$ where -1 in $\chi(-1)$ stands for complex conjugation. ∎

3.6. Using the main conjecture of Iwasawa theory for imaginary quadratic fields. We recall the definition of the plus/minus norm subgroups (Definition 2.11).

Definition 3.13 (Plus/minus Selmer group).

$$\mathrm{Sel}_{R_p}^{\pm}(E/F_{\mathrm{cyc}}) := \ker\left(\mathrm{Sel}_{R_p}(E/F_{\mathrm{cyc}}) \to \prod_{a\in S} \frac{H^1(F_{\mathrm{cyc},a}, \mathbf{A})}{\hat{E}^{\pm}(F_{\mathrm{cyc},a}) \otimes R_p} \right).$$

For an R_p-module M let $M^\vee$ be the R_p-Pontryagin dual $\mathrm{Hom}_{R_p}(M, D_p)$.

PROPOSITION 3.14. *We have*

$$\hat{E}^{\pm}(F_{\mathrm{cyc},a}) \otimes_O D_p^\vee \cong \mathcal{U}^{\kappa}_{F_{\mathrm{cyc},a}}/\tilde{V}_a^{\pm},$$
$$\hat{E}^{\pm}(F_{\mathrm{cyc},a}) \otimes_{O,\phi} D_p^\vee \cong \mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc},a}}/\tilde{V}_a^{\pm,\prime}$$

for some $\tilde{V}_a^{\pm}$ *and* $\tilde{V}_a^{\pm,\prime}$.

Proof. Obvious. ∎

Let $\tilde{V}^{\pm} := \prod_{a\in S} \tilde{V}_a^{\pm}$ and $\tilde{V}^{\pm,\prime} := \prod_{a\in S} \tilde{V}_a^{\pm,\prime}$. Let $\alpha : \mathcal{U} \to X$ be the Artin map of global class field theory. The following is clear.

PROPOSITION 3.15.

$$\mathrm{Sel}^{\pm}_{R_p}(E/F_{\mathrm{cyc}}) \cong \mathrm{Hom}_O(X^{\kappa}_{F_{\mathrm{cyc}}}/\alpha(\tilde{V}^{\pm}), D_p) \oplus \mathrm{Hom}_O(X^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/\alpha(\tilde{V}^{\pm,\prime}), D_p).$$

Proof. This follows from

$$\mathrm{Sel}_p(E/K(\mathfrak{f}p^\infty)) \cong \mathrm{Hom}(X, E[p^\infty])$$

(see [6, 4.1, p. 124]). ∎

PROPOSITION 3.16.

(i) $\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}$ *and* $\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}$ *are free of rank* $2d$ *over* Λ_{R_p}.
(ii) (*For the plus part, assume* $\varphi(p) \not\equiv p \pmod{p^2}$.) $\tilde{V}^{\pm}$, $\tilde{V}^{\pm,\prime}$, $\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm}$, *and* $\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm,\prime}$ *are free of rank* d *over* Λ_{R_p}.

Proof. (i) is from [7]; (ii) follows from Proposition 3.3. ∎

PROPOSITION 3.17.

(i) $\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}}$ *and* $\mathcal{C}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}$ *are free of rank* d *over* Λ_{O_p}.
(ii) *The maps* $\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}} \to \mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}$ *and* $\mathcal{C}^{\bar{\kappa}}_{F_{\mathrm{cyc}}} \to \mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}$ *are injective.*

Proof. (i) is [23, Theorem 7.7] (see also Proposition 3.9).

Let $\theta_\phi = \sum_{\mathfrak{a}\subset O_K} \phi(\mathfrak{a}) q^{N\mathfrak{a}}$ be the theta series of a Hecke character ϕ of K of weight $(1,0)$ (and therefore a newform of weight 2 and certain level and character). We note $L(\bar{\varphi}, \eta\chi, 1)$ $(= L(\theta_{\bar{\varphi}\eta}, \chi, 1))$ and $L(\varphi, \eta\chi, 1)$ $(= L(\theta_{\varphi\eta}, \chi, 1))$ are non-vanishing for all but finitely many characters χ of $\mathrm{Gal}(F_{\mathrm{cyc}}/F)$, by Rohrlich [20]. Then (ii) follows from Proposition 3.12 and (i). ∎

The following proposition follows from the main conjecture for quadratic imaginary fields [21].

PROPOSITION 3.18. (*Again, for the plus part, assume* $\varphi(p) \not\equiv p \pmod{p^2}$.)

$$\mathrm{char}_{\Lambda_{R_p}}(X^{\kappa}_{F_{\mathrm{cyc}}}/\alpha(\tilde{V}^{\pm})) = \mathrm{char}_{\Lambda_{R_p}}(\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}/(\tilde{V}^{\pm} + \mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}})),$$
$$\mathrm{char}_{\Lambda_{R_p}}(X^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/\alpha(\tilde{V}^{\pm,\prime})) = \mathrm{char}_{\Lambda_{R_p}}(\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/(\tilde{V}^{\pm,\prime} + \mathcal{C}^{\bar{\kappa}}_{F_{\mathrm{cyc}}})).$$

In other words,

$$\begin{aligned}&\mathrm{char}_{\Lambda_{R_p}}(\mathrm{Sel}^{\pm}_{R_p}(E/F_{\mathrm{cyc}})^{\vee})\\&\quad=\mathrm{char}_{\Lambda_{R_p}}(\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}/(\tilde{V}^{\pm}+\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}}))\cdot\mathrm{char}_{\Lambda_{R_p}}(\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/(\tilde{V}^{\pm,\prime}+\mathcal{C}^{\bar{\kappa}}_{F_{\mathrm{cyc}}})).\end{aligned}$$

We let $L_{/F}(E,\bar{\chi},s)$ denote the (Hasse–Weil) L-function of E over F twisted by $\bar{\chi}$ with terms not prime to $\mathfrak{f}p$ removed. In other words, considering χ as a Dirichlet character and supposing $\sum_n a_n/n^s$ is the Hasse–Weil L-function of E over F, we let $L_{/F}(E,\bar{\chi},s):=\sum_{n,\,(n,\mathfrak{f}p)=1}a_n\bar{\chi}(n)/n^s$. By the above discussion combined with Proposition 3.12, we obtain

THEOREM 3.19. (*For f^+, assume $\varphi(p)\not\equiv p \pmod{p^2}$.*) *We have $(f^{\pm})=\mathrm{char}_{\Lambda_{R_p}}(\mathrm{Sel}^{\pm}_{R_p}(E/F_{\mathrm{cyc}})^{\vee})$ for some $f^{\pm}\in\Lambda_{R_p}$ such that for every primitive character χ of $\mathrm{Gal}(F_n/F)$ with $(-1)^n=\epsilon$,*

$$\chi(f^{\epsilon})=\left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^{-\epsilon})}\right)^{2[F:K]}\frac{L_{/F}(E,\bar{\chi},1)}{(\Omega_E\overline{\Omega}_E)^{[F:K]}}.$$

Proof. From Proposition 3.14 we have

$$\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm}\cong\prod_{a\in S}\mathrm{Hom}_O(\hat{E}^{\pm}(F_{\mathrm{cyc},a})\otimes_O D_p,D_p),\tag{3.2}$$

$$\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm,\prime}\cong\prod_{a\in S}\mathrm{Hom}_O(\hat{E}^{\pm}(F_{\mathrm{cyc},a})\otimes_{O,\phi} D_p,D_p).\tag{3.3}$$

Let $\varphi^{\pm}$ be the image of ξ under (3.2), and $\varphi^{\pm,\prime}$ the image of ξ under (3.3).

Recall $f^{\pm}_{\eta}$ and $f^{\pm,\prime}_{\eta}$ from Proposition 3.3. For some $h^{\pm}_{\eta},h^{\pm,\prime}_{\eta}\in\Lambda_{O_p}$ we have

$$\varphi^{\pm}=\sum_{\eta}h^{\pm}_{\eta}f^{\pm}_{\eta},\qquad\varphi^{\pm,\prime}=\sum_{\eta}h^{\pm,\prime}_{\eta}f^{\pm,\prime}_{\eta},$$

and $\mathrm{char}(\mathcal{U}^{\kappa}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm}+\mathcal{C}^{\kappa}_{F_{\mathrm{cyc}}})\cong\prod_{\eta}h^{\pm}_{\eta}$ and $\mathrm{char}(\mathcal{U}^{\bar{\kappa}}_{F_{\mathrm{cyc}}}/\tilde{V}^{\pm,\prime}+\mathcal{C}^{\bar{\kappa}}_{F_{\mathrm{cyc}}})\cong\prod_{\eta}h^{\pm,\prime}_{\eta}$.

For every non-trivial character $\chi:\mathrm{Gal}(F_n/F)\to\bar{\mathbb{Q}}^{\times}$ and any n, we have

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)\varphi^{\pm}(d^{\pm\sigma}_{n,\eta}\otimes p^{-k})=\chi(h^{\pm}_{\eta})\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)f^{\pm}_{\eta}(d^{\pm\sigma}_{n,\eta}\otimes p^{-k}),$$

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)\varphi^{\pm,\prime}(\bar{d}^{\pm\sigma}_{n,\eta}\otimes p^{-k})=\chi(h^{\pm,\prime}_{\eta})\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)f^{\pm,\prime}_{\eta}(\bar{d}^{\pm\sigma}_{n,\eta}\otimes p^{-k}).$$

We can compute the left-hand sides using Proposition 3.12:

$$\begin{aligned}&\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)\varphi^{\pm}(d^{\pm\sigma}_{n,\eta}\otimes p^{-k})\\&\quad=-p^{-k}12[Nb-\varphi(b)\chi(\sigma_b)\eta^{-1}(\sigma_b|_F)]\frac{L(\bar{\varphi},\eta\bar{\chi},1)}{\Omega_E}\left[\frac{\rho}{p}\right]^{[(n+1)/2]}\tau_{n+1}(\chi),\end{aligned}$$

and similarly,

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)\varphi^{\pm,\prime}(\bar{d}_{n,\eta}^{\pm\sigma}\otimes p^{-k})$$
$$=-p^{-k}12[Nb-\bar{\varphi}(b)\chi(\sigma_b)\eta^{-1}(\sigma_b|_F)]\frac{L(\varphi,\eta\bar{\chi},1)}{\overline{\Omega}_E}\left[\frac{\bar{\rho}}{p}\right]^{[(n+1)/2]}\tau_{n+1}(\chi).$$

On the other hand, from Proposition 3.3 we have

$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)f_\eta^{\pm}(d_{n,\eta}^{\pm\sigma}\otimes p^{-k})=\chi(\tilde{\omega}_n^{\mp})p^{-k},$$
$$\sum_{\sigma\in\mathrm{Gal}(F_n/F)}\chi(\sigma)f_\eta^{\pm,\prime}(\bar{d}_{n,\eta}^{\pm\sigma}\otimes p^{-k})=\chi(\tilde{\omega}_n^{\mp})p^{-k}.$$

Thus

$$\chi(h_\eta^{\pm})$$
$$=-12[Nb-\varphi(b)\chi(\sigma_b)\eta^{-1}(\sigma_b|_F)]\frac{L(\bar{\varphi}\eta\overline{\chi},1)}{\Omega_E}\left[\frac{\rho}{p}\right]^{[(n+1)/2]}\tau_{n+1}(\chi)/\chi(\tilde{\omega}_n^{\mp}),$$
$$\chi(h_\eta^{\pm,\prime})$$
$$=-12[Nb-\bar{\varphi}(b)\chi(\sigma_b)\eta^{-1}(\sigma_b|_F)]\frac{L(\varphi\eta\overline{\chi},1)}{\overline{\Omega}_E}\left[\frac{\bar{\rho}}{p}\right]^{[(n+1)/2]}\tau_{n+1}(\chi)/\chi(\tilde{\omega}_n^{\mp}).$$

Let $g_\eta(X):=Nb-\varphi(b)\eta^{-1}(\sigma_b|_F)\sigma_b$ and $\bar{g}_\eta(X):=Nb-\bar{\varphi}(b)\eta^{-1}(\sigma_b|_F)\sigma_b$. Since $\rho\cdot\bar{\rho}=N_{K/\mathbb{Q}}\rho=p^2$, it follows that

$$\chi(f^\epsilon)=\left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^{-\epsilon})}\right)^{2[F:K]}\prod_\eta\chi(g_\eta(X))\chi(\bar{g}_\eta(X))\frac{L(\bar{\varphi}\eta\bar{\chi},1)L(\varphi\eta\bar{\chi},1)}{\Omega_E\overline{\Omega}_E}$$
$$=\left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^{-\epsilon})}\right)^{2[F:K]}\frac{L_{/F}(E,\bar{\chi},1)}{(\Omega_E\overline{\Omega}_E)^d}\prod_\eta\chi(g_\eta(X))\chi(\bar{g}_\eta(X)).$$

(The second line is obtained from the first by the Artin formalism of L-functions, and also because the terms not prime to $\mathrm{disc}(F/K)$ are removed in the definition of $L_{/F}(E,\bar{\chi},s)$.)

Furthermore, we can make the following point: Since we assumed that $b=(x_b)$ splits completely over $K(f)/K$ and $x_b\not\equiv 0,1 \pmod p$, we have $\eta(\sigma_b|_F)=1$ for every η and $g_\eta(X)\equiv Nb-x_b \pmod{(X)}$ and $\bar{g}_\eta(X)\equiv Nb-\bar{x_b} \pmod{(X)}$, which are units in Λ_{R_p}. Thus our theorem follows. ∎

4. Analytic plus/minus p-adic L-functions. We keep the notation of the previous sections. Recall that E is an elliptic curve over F with CM by $\mathcal{O}_K$. The goal of this section is to construct the analytic plus/minus p-adic L-functions of E/F for a supersingular prime p using the idea of [18].

4.1. Pollack's supersingular p-adic L-functions. R. Pollack [18] constructed the plus/minus p-adic L-function $L_p^{\pm}(f,T)$ belonging to the Iwasawa algebra for a Hecke eigenform f at a supersingular prime p in the case where its pth Hecke eigenvalue (pth Fourier coefficient) is 0. We briefly review his construction for weight 2 Hecke eigenforms.

Let f be a Hecke eigenform of weight 2, level N, and character ϵ whose nth Hecke eigenvalue is a_n. Let K_f be the number field generated by a_n and the values of ϵ; let $\mathcal{O}_f$ denote its ring of integers. The periods of f are defined by

$$\phi(f,r) := 2\pi i \int_{i\infty}^{r} f(z)\,dz$$

for $r \in \mathbb{Q}$. Let $\eta(f;a,m) := \phi(f,a/m)$ and fix the positive and negative parts of $\eta(f;a,m)$ by setting

$$\eta^{\pm}(f;a,m) := \frac{\eta(f;a,m) \pm \eta(f;-a,m)}{2}.$$

The well-known theorem of Shimura and Manin (see [18, Theorem 2.7] for example) says there exist two non-zero complex numbers Ω_f^+ and Ω_f^- such that

$$\frac{\eta^{\pm}(f;a,m)}{\Omega_f^{\pm}} \in \mathcal{O}_f$$

for all $a, m \in \mathbb{Z}$. Let $\mathrm{ord}_p(\cdot)$ be the valuation satisfying $\mathrm{ord}_p(p) = 1$. Call a root α of the pth Frobenius polynomial $x^2 - a_p x + \epsilon(p)p = 0$ *allowable* if $\mathrm{ord}_p(\alpha) < 1$. For a fixed allowable root α, one can define two h-admissible measures ($h = \mathrm{ord}_p(\alpha)$) on $\mathbb{Z}_p^{\times}$ by the formulas (see [18, Proposition 2.8])

$$\mu_{f,\alpha}^{\pm}(a + p^n\mathbb{Z}_p) = \frac{1}{\alpha^n} \cdot \frac{\eta^{\pm}(f;a,p^n)}{\Omega_f^{\pm}} - \frac{\epsilon(p)}{\alpha^{n+1}} \cdot \frac{\eta^{\pm}(f;a,p^{n-1})}{\Omega_f^{\pm}}$$

where a is prime to p. Then the p-adic L-function of f with respect to an allowable root α is defined to be

$$L_p(f,\alpha,\chi) := \int_{\mathbb{Z}_p^{\times}} \chi(x)\,d\mu_{f,\alpha}^{\pm}(x) = \mu_{f,\alpha}^{\pm}(\chi)$$

for $\chi \in \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^{\times}, \mathbb{C}_p^{\times})$, using the fact that locally analytic functions are integrable with respect to an h-admissible measure. We call characters on $\mathbb{Z}_p^{\times} \simeq (\mathbb{Z}/p\mathbb{Z})^{\times} \times (1 + p\mathbb{Z}_p)$ *tame* if they factor through $(\mathbb{Z}/p\mathbb{Z})^{\times}$, and *wild* if they factor through $1 + p\mathbb{Z}_p$. By the theorem of Vishik [32, Theorem 2.3], $L_p(f,\alpha,\chi)$ is analytic in χ, and hence we can form its power series expansion about a tame character χ. We denote this power series by $L_p(f,\alpha,\chi,T)$. Then for $u \in \mathbb{C}_p^{\times}$ with $|u-1|_p < 1$ we have

$$L_p(f,\alpha,\chi,u-1) = L_p(f,\alpha,\chi\chi_u)$$

where χ_u is the wild character sending the topological generator γ of $1+p\mathbb{Z}_p$ to $u \in \mathbb{C}_p^\times$. If the tame character χ is trivial, then we write $L_p(f,\alpha,T)$ for $L_p(f,\alpha,\chi,T)$. The p-adic L-functions depend upon a choice of complex periods $\Omega_f^\pm$, which are defined only up to an element of $\mathcal{O}_f$. Let $\Phi_n(T) := \sum_{t=0}^{p-1} T^{p^{n-1}\cdot t}$ be the p^nth cyclotomic polynomial. Define

$$\log_p^+(T) := \frac{1}{p}\cdot\prod_{n=1}^{\infty}\left(\frac{\Phi_{2n}(1+T)}{p}\right),$$
$$\log_p^-(T) := \frac{1}{p}\cdot\prod_{n=1}^{\infty}\left(\frac{\Phi_{2n-1}(1+T)}{p}\right),$$

which are known to be in $\mathbb{Q}_p[[T]]$ and to converge on the open unit disc centered at 0 [18, Lemma 4.1]. Let $K_{f,p}$ be the completion of K_f at a chosen prime ideal above p; let $\mathcal{O}_{K_{f,p}}$ denote its ring of integers. Note that if p is a supersingular prime then $L_p(f,\alpha,T)$ does not belong to the Iwasawa algebra. But thanks to Pollack, we have analytic plus/minus p-adic L-functions for supersingular prime p which are actually elements of the Iwasawa algebra. The main Theorem 5.1 of [18] is

THEOREM 4.1 (Pollack). *If p is odd and $a_p = 0$, then there exist $L_p^\pm(f,T) \in \mathcal{O}_{K_{f,p}}[[T]]\otimes K_{f,p}$ such that*

$$L_p(f,\alpha,T) = L_p^+(f,T)\cdot\log_p^+(T) + L_p^-(f,T)\cdot\log_p^-(T)\cdot\alpha.$$

It turns out (since $a_p = 0$, two allowable roots are α and $-\alpha$) that

$$L_p^+(f,T) = \frac{L_p(f,\alpha,T)+L_p(f,-\alpha,T)}{2\log_p^+(T)},$$
$$L_p^-(f,T) = \frac{L_p(f,\alpha,T)-L_p(f,-\alpha,T)}{2\alpha\log_p^-(T)}.$$

4.2. Application to CM elliptic curves over F. Now we apply Pollack's construction to our setting. Let $\mathbf{f}$ (a non-zero ideal of F) be the conductor of E/F. By the main theorem of complex multiplication, one can attach an algebraic Hecke character ψ of conductor $\mathbf{f}$ to E/F which has the following property:

$$L(E/F,s) = L(\psi,s)\cdot L(\overline{\psi},s)$$

where $\overline{\psi}$ is the complex conjugation of ψ. Due to our running assumption (see Section 3.1), we have $\psi = \varphi\circ N_{F/K}$ so that

$$L(\psi,s) = \prod_{\eta\in\widehat{\mathrm{Gal}(F/K)}} L(\eta\varphi,s)$$

where $\widehat{\mathrm{Gal}(F/K)}$ is the set of characters of $\mathrm{Gal}(F/K)$. Let $\theta_{\eta\varphi}$ be the CM modular form associated to $\eta\varphi$ given by

$$\theta_{\eta\varphi}(z) := \sum_{\substack{A\subset K\\(A,\mathbf{f}_{\eta\varphi})=1}} \eta(\sigma_A)\varphi(A)q^{\mathrm{Norm}(A)} = \sum_{n=1}^{\infty} a_n(\eta\varphi)q^n \quad \text{with} \quad q = e^{2\pi iz}$$

where the sum is over integral ideals of K prime to $\mathbf{f}_{\eta\varphi} = \text{l.c.m.}\{\mathbf{f}_\varphi, \mathbf{f}_\eta\}$, and $\sigma_A \in \mathrm{Gal}(F/K)$ is the image $[A, F/K]$ of the Artin reciprocity map. Then, by Hecke (see [25, p. 141]), $\theta_{\eta\varphi}$ is a weight 2 Hecke (new) eigenform for $\Gamma_0(N)$ where $N = D\cdot\mathrm{Norm}(\mathbf{f}_{\eta\varphi})$, with the nebentypus character $\epsilon_{\eta\varphi}$ given by

$$\epsilon_{\eta\varphi}(\ell) := \left(\frac{D}{\ell}\right)\cdot\frac{\eta\varphi(\ell\mathcal{O}_K)}{\ell} = \left(\frac{D}{\ell}\right)\cdot\frac{\eta(\sigma_{\ell\mathcal{O}_K})\varphi(\ell\mathcal{O}_K)}{\ell}$$

for every prime $\ell\nmid N$ where $(\frac{D}{\cdot})$ is the quadratic character associated to K. Note $a_1(\eta\varphi) = 1$. This normalized Hecke eigenform $\theta_{\eta\varphi}$ provides the modularity of the Hecke character $\eta\varphi$ in the sense that

$$L(\eta\varphi, s) = L(\theta_{\eta\varphi}, s) := \sum_{n\geq 1}\frac{a_n(\eta\varphi)}{n^s}. \tag{4.1}$$

Let p be an odd prime inert in K which is prime to $\mathbf{f}$, which in turn implies $a_p(\eta\varphi) = 0$ for any $\eta\in\widehat{\mathrm{Gal}(F/K)}$ (so p is a supersingular prime for E/F). Let $\alpha_1(\eta\varphi)$ and $\alpha_2(\eta\varphi)$ be allowable (i.e., $h_i = \mathrm{ord}_p(\alpha_i(\eta\varphi)) < 1$ for $i = 1, 2$) roots of $x^2 - a_p(\eta\varphi)x + \epsilon_{\eta\varphi}(p)p = 0$. So we have $\alpha_1(\eta\varphi) = -\alpha_2(\eta\varphi) = \overline{\alpha_2(\eta\varphi)}$ and $-\alpha_1(\eta\varphi)^2 = \epsilon_{(\eta\varphi)}(p)p = -\varphi(p\mathcal{O}_K)$, since $\eta(\sigma_{p\mathcal{O}_K}) = 1$. In other words, $\alpha_1(\eta\varphi)^2 = \rho$ where $\rho := \varphi(p\mathcal{O}_K)$. Note that [27, Corollary 10.4.1] tells us

$$p^2 = N_{K/\mathbb{Q}}(\rho) = \rho\cdot\bar{\rho}.$$

We record one of the properties of the p-adic L-function $L_p(\theta_{\eta\varphi}, \alpha_1(\eta\varphi), T)$:

$$L_p(\theta_{\eta\varphi}, \alpha_1(\eta\varphi), \zeta_{p^n} - 1) = \begin{cases} L_p(\theta_{\eta\varphi}, -\alpha_1(\eta\varphi), \zeta_{p^n} - 1), & n \text{ odd},\\ -L_p(\theta_{\eta\varphi}, -\alpha_1(\eta\varphi), \zeta_{p^n} - 1), & n \text{ even}.\end{cases}$$

Let χ be a finite order character on $\mathbb{Z}_p^\times$ of conductor p^{n+1} whose tame part is trivial. Then using [18, Proposition 2.11] and the above remarks, we compute, for any odd positive integer n,

$$\begin{aligned} L_p^+(\theta_{\eta\varphi}, \zeta_{p^n} - 1) &= \frac{1}{\alpha_1(\eta\varphi)^{n+1}}\cdot\frac{p^{n+1}}{\tau_{n+1}(\chi^{-1})}\cdot\frac{L(\theta_{\eta\varphi}, \chi^{-1}, 1)}{\Omega^+_{\theta_{\eta\varphi}}}\cdot\frac{1}{\log_p^+(\zeta_{p^n} - 1)}\\ &= \frac{\tau_{n+1}(\chi)}{\alpha_1(\eta\varphi)^{n+1}}\cdot\frac{L(\theta_{\eta\varphi}, \chi^{-1}, 1)}{\Omega^+_{\theta_{\eta\varphi}}}\cdot\frac{1}{\log_p^+(\zeta_{p^n} - 1)}\end{aligned}$$

$$= \frac{\tau_{n+1}(\chi)}{\rho^{(n+1)/2}} \cdot \frac{L(\theta_{\eta\varphi}, \bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\varphi}}} \cdot \frac{p^{(n+1)/2}}{\prod_{j=1}^{(n-1)/2} \Phi_{2j}(\zeta_{p^n})}$$
$$= \frac{\tau_{n+1}(\chi)}{\rho^{(n+1)/2}} \cdot \frac{L(\eta\varphi\bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\varphi}}} \cdot \frac{p^{(n+1)/2}}{\chi(\tilde{\omega}^+_n)}$$

where $\tau_{n+1}(\chi^{-1}) = \sum_{\sigma\in(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} \chi^{-1}(\sigma)\zeta^\sigma_{p^{n+1}}$ is the Gauss sum which satisfies $\tau_{n+1}(\chi^{-1})\cdot\tau_{n+1}(\chi) = \overline{\tau_{n+1}(\chi)}\cdot\tau_{n+1}(\chi) = p^{n+1}$. Here we have also used the interpolation property [18, Lemma 4.7]

$$\log^+_p(\zeta_{p^n} - 1) = \begin{cases} p^{-(n+1)/2} \prod_{j=1}^{(n-1)/2} \Phi_{2j}(\zeta_{p^n}) & \text{for } n \text{ odd}, \\ 0 & \text{otherwise}, \end{cases}$$

and

$$L(\eta\varphi\bar{\chi}, 1) = L(\theta_{\eta\varphi}, \bar{\chi}, 1) \quad \text{and} \quad \chi(\tilde{\omega}^+_n) = \prod_{j=1}^{(n-1)/2} \Phi_{2j}(\zeta_{p^n}) \quad \text{for } n \text{ odd}.$$

(Note that the modularity (4.1) implies that $L(\eta\varphi\bar{\chi}, s)$ is the L-function of a Hecke character of K, and $L(\theta_{\eta\varphi}, \bar{\chi}, s)$ is the L-function of a modular form twisted by $\bar{\chi}$.) Similarly, $\theta_{\eta\bar{\varphi}}$ is also a weight 2 Hecke eigenform. So a similar computation yields

$$L^+_p(\theta_{\eta\bar{\varphi}}, \zeta_{p^n} - 1) = \frac{\tau_{n+1}(\chi)}{\bar{\rho}^{(n+1)/2}} \cdot \frac{L(\eta\bar{\varphi}\bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\bar{\varphi}}}} \cdot \frac{p^{(n+1)/2}}{\chi(\tilde{\omega}^+_n)}$$

for n odd positive. Using the fact $\rho\bar{\rho} = p^2$, we get, for odd positive n

$$L^+_p(\theta_{\eta\varphi}, \zeta_{p^n} - 1) \cdot L^+_p(\theta_{\eta\bar{\varphi}}, \zeta_{p^n} - 1) = \frac{L(\eta\varphi\bar{\chi}, 1) \cdot L(\eta\bar{\varphi}\bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\varphi}} \cdot \Omega^+_{\theta_{\eta\bar{\varphi}}}} \cdot \left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}^+_n)}\right)^2.$$

We compute the minus p-adic analytic functions of $\theta_{\eta\varphi}$ and $\theta_{\eta\bar{\varphi}}$ similarly:

$$L^-_p(\theta_{\eta\varphi}, \zeta_{p^n} - 1) = \frac{\tau_{n+1}(\chi)}{\rho^{(n+2)/2}} \cdot \frac{L(\eta\varphi\bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\varphi}}} \cdot \frac{p^{(n+2)/2}}{\chi(\tilde{\omega}^-_n)},$$
$$L^-_p(\theta_{\eta\bar{\varphi}}, \zeta_{p^n} - 1) = \frac{\tau_{n+1}(\chi)}{\bar{\rho}^{(n+2)/2}} \cdot \frac{L(\eta\bar{\varphi}\bar{\chi}, 1)}{\Omega^+_{\theta_{\eta\bar{\varphi}}}} \cdot \frac{p^{(n+2)/2}}{\chi(\tilde{\omega}^-_n)}$$

for n even positive because

$$\log^-_p(\zeta_{p^n} - 1) = \begin{cases} p^{-(n+2)/2} \cdot \prod_{j=1}^{n/2} \Phi_{2j-1}(\zeta_{p^n}) & \text{for } n \text{ even}, \\ 0 & \text{otherwise}, \end{cases}$$

and

$$\chi(\tilde{\omega}^-_n) = \prod_{j=1}^{n/2} \Phi_{2j-1}(\zeta_{p^n}) \quad \text{for } n \text{ even positive}.$$

Therefore

$$L_p^-(\theta_{\eta\varphi},\zeta_{p^n}-1)\cdot L_p^-(\theta_{\eta\bar{\varphi}},\zeta_{p^n}-1)=\frac{L(\eta\varphi\bar{\chi},1)\cdot L(\eta\bar{\varphi}\bar{\chi},1)}{\Omega^+_{\theta_{\eta\varphi}}\cdot\Omega^+_{\theta_{\eta\bar{\varphi}}}}\cdot\left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^-)}\right)^2$$

for n even. Consequently, we have the following interpolation properties:

$$\prod_{\eta\in\widehat{\mathrm{Gal}(F/K)}} L_p^\epsilon(\theta_{\eta\varphi},\zeta_{p^n}-1)\cdot L_p^\epsilon(\theta_{\eta\bar{\varphi}},\zeta_{p^n}-1) = \left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^\epsilon)}\right)^{2[F:K]}\frac{L(E/F,\bar{\chi},1)}{\prod_\eta \Omega^+_{\theta_{\eta\varphi}}\cdot\Omega^+_{\theta_{\eta\bar{\varphi}}}}$$

for every primitive character χ of $\mathrm{Gal}(F_n/F)$ with $(-1)^{n+1}=\epsilon$ (ϵ is the parity of $\pm$).

Note that by the theorem of Rohrlich [20], there are only a finite number of characters χ of p-power order and conductor such that $L(\theta_{\eta\varphi},\chi,1)=0$, guaranteeing that the p-adic L-functions $L_p^\pm$ are not identically zero.

Let $\mathcal{K}$ be be the composite of the fields $K_{\theta_{\eta\varphi}}$ and $K_{\theta_{\eta\bar{\varphi}}}$, and let $\mathcal{K}_p$ be the completion of $\mathcal{K}$ at a chosen prime ideal above p. We denote by $\mathcal{O}_{\mathcal{K}_p}$ the ring of integers of $\mathcal{K}_p$. We now define the analytic plus/minus p-adic L-function $L^\pm(E/F,T)$ of our CM elliptic curve E/F:

Definition 4.2 (Plus/minus p-adic L-function for E/F).

$$L_p^\pm(E/F,T):=\prod_{\eta\in\widehat{\mathrm{Gal}(F/K)}} L_p^\pm(\theta_{\eta\varphi},T)\cdot L_p^\pm(\theta_{\eta\bar{\varphi}},T)\in\mathcal{O}_{\mathcal{K}_p}[[T]]\otimes\mathcal{K}_p.$$

Note that $L_p^\pm(E/F,T)$ depends on the choice of complex periods, and from now on we fix these periods as follows;

$$\Omega^+_{\theta_{\eta\varphi}}=\Omega_E \quad\text{and}\quad \Omega^+_{\theta_{\eta\bar{\varphi}}}=\overline{\Omega}_E \quad\text{for every } \eta\in\mathrm{Gal}(F/K).$$

5. Main conjecture for CM elliptic curves. In this section we compare the analytic p-adic L-function with the algebraic p-adic L-function to prove the main conjecture. Recall that $\mathbf{f}$ (a non-zero ideal of F) is the conductor of E over F. Also recall that there exist Hecke characters ψ of F and φ of K such that

$$\psi=\varphi\circ N_{F/K},$$

and $\mathfrak{f}$ is an integral ideal of K divisible by $\mathrm{cond}(F/K)$ and by $\mathfrak{f}_\varphi:=\mathrm{cond}(\varphi)$.

Theorem 5.1 (Iwasawa main conjecture). *Assume* $\mathbf{f}\cap\mathcal{O}_K=\mathfrak{f}$. *Then*

$$\mathrm{char}_{\Lambda_{R_p}}(\mathrm{Sel}^-_{R_p}(E/F_{\mathrm{cyc}})^\vee)=(L_p^+(E/F,T))$$

in $R_p[[T]]$. *Assuming* $\varphi(p)\not\equiv p \pmod{p^2}$, *we have*

$$\mathrm{char}_{\Lambda_{R_p}}(\mathrm{Sel}^+_{R_p}(E/F_{\mathrm{cyc}})^\vee)=(L_p^-(E/F,T)).$$

Proof. By Theorem 3.19 we have $\mathrm{char}_{\Lambda_{R_p}}(\mathrm{Sel}^{\pm}_{R_p}(E/F_{\mathrm{cyc}})^{\vee}) = (f^{\pm})$ for $f^{\pm} \in \Lambda_{R_p} \simeq R_p[[T]]$. For every primitive character χ of $\mathrm{Gal}(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$ with n odd we can prove, by the previous interpolation formulas,

$$\chi(f^-) = \left(\frac{\tau_{n+1}(\chi)}{\chi(\tilde{\omega}_n^+)}\right)^{2[F:K]} \frac{L(E/F,\bar{\chi},1)}{(\Omega_E\overline{\Omega}_E)^{[F:K]}} = \chi(L_p^+(E/F,T)),$$

which implies $(f^-) = (L_p^+(E/F,T))$. Similarly we can show that $(f^+) = (L_p^-(E/F,T))$, which completes the proof. ∎

Remark 5.2. Pollack's Theorem 4.1 says that

$$L_p^{\pm}(E/F,T) \in R_p[[T]] \otimes \mathrm{Frac}(R_p).$$

Our Theorem 5.1 implies

$$L_p^{\pm}(E/F,T) \in R_p[[T]]$$

under our choice of periods.

Acknowledgements. Byoung Du Kim was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2014R1A2A2A01002549).

Jeehoon Park was partially supported by Basic Science Research Program (2013023108) and Priority Research Centers Program (2013053914) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology.

References

[1] K. Büyükboduk, *On the Iwasawa theory of CM fields for supersingular primes*, Trans. Amer. Math. Soc. 370 (2018), 927–966.

[2] K. Büyükboduk and A. Lei, *Coleman-adapted Rubin–Stark Kolyvagin systems and supersingular Iwasawa theory of CM abelian varieties*, Proc. London Math. Soc. 111 (2015), 1338–1378.

[3] K. Büyükboduk and A. Lei, *Integral Iwasawa theory of Galois representations for non-ordinary primes*, Math. Z. 286 (2017), 361–398.

[4] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. 124 (1996), 129–174.

[5] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.

[6] E. de Shalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Perspectives Math. 3, Academic Press, Boston, MA, 1987.

[7] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. 47 (1978), 85–99.

[8] R. Greenberg, *Iwasawa theory for elliptic curves*, in: Arithmetic Theory of Elliptic Curves (Cetraro, 1997), C. Viola (ed.), Lecture Notes in Math. 1716, Springer, 1999, 51–144.

[9] M. Hazewinkel, *On norm maps for one dimensional formal groups. I. The cyclotomic Γ-extension*, J. Algebra 32 (1974), 89–108.
[10] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan 22 (1970), 213–246.
[11] B. Im and B. Kim, *Ranks of rational points of the Jacobian varieties of hyperelliptic curves*, arXiv:1702.07837 (2017).
[12] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over number fields*, J. Reine Angew. Math. 598 (2006), 71–103.
[13] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in: Cohomologies p-adiques et applications arithmétiques. III, Astérisque 295 (2004), ix, 117–290.
[14] B. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. 143 (2007), 47–72.
[15] T. Kitajima and R. Otsuki, *On the plus and the minus Selmer groups for elliptic curves at supersingular primes*, arXiv:1607.03612 (2016).
[16] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. 152 (2003), 1–36.
[17] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. 25 (1974), 1–61.
[18] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. 118 (2003), 523–558.
[19] R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. 159 (2004), 447–464.
[20] D. Rohrlich, *L-functions and division towers*, Math. Ann. 281 (1988), 611–632.
[21] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.
[22] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 64 (1981), 455–470.
[23] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in: Arithmetic Theory of Elliptic Curves (Cetraro, 1997), C. Viola (ed.), Lecture Notes in Math. 1716, Springer, New York, 1999, 167–234.
[24] K. Rubin, *Local units, elliptic units, Heegner points, and elliptic curves*, Invent. Math. 88 (1987), 405–422.
[25] N. Schappacher, *Periods of Hecke Characters*, Lecture Notes in Math. 1301, Springer, 1988.
[26] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, 1971.
[27] J. Silverman, *Advanced Topics on the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.
[28] C. Skinner and E. Urban, *The Iwasawa main conjectures for GL_2*, Invent. Math. 195 (2014), 1-277.
[29] F. Sprung, *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*, J. Number Theory 132 (2012), 1483–1506.
[30] F. Sprung, *On pairs of p-adic L-functions for weight-two modular forms*, Algebra Number Theory 11 (2017), 885–928.
[31] F. Sprung, *The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes*, submitted.
[32] M. M. Vishik, *Nonarchimedean measures associated with Dirichlet series*, Mat. Sb. (N.S.) 99 (141) (1976), 248–260, 296 (in Russian).

[33] X. Wan, *Iwasawa Main Conjecture for supersingular elliptic curves*, arXiv:1411.6352 (2014).
[34] A. Wiles, *Higher explicit reciprocity laws*, Ann. of Math. (2) 107 (1978), 235–254.

Byoung Du Kim
School of Mathematics and Statistics
Victoria University of Wellington
Wellington 6140, New Zealand
E-mail: byoungdu.kim@vuw.ac.nz

Jeehoon Park
Department of Mathematics
Pohang University of Science and Technology
77 Cheongam-Ro, Namgu
Pohang, Gyeongbuk, 37673, South Korea
E-mail: jeehoonpark@postech.ac.kr